Department of Homeland Security

Office of Inspector General

Information Technology Management Letter for the United States Coast Guard Component of the FY 2013 Department of Homeland Security's Financial Statement Audit

OIG-14-88

May 2014

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

May 2, 2014

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

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

FROM: Richard Harsche
Acting Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the United States Coast Guard Component of the FY 2013 Department of Homeland Security's Financial Statement Audit*

Attached for your information is our final report, *Information Technology Management Letter for the United States Coast Guard Component of the FY 2013 Department of Homeland Security's Financial Statement Audit.* This report contains comments and recommendations related to information technology internal control deficiencies that were not required to be reported in the Independent Auditors' Report.

We contracted with the independent public accounting firm KPMG LLP (KPMG) to conduct the audit of Department of Homeland Security fiscal year 2013 consolidated financial statements. The contract required that KPMG perform its audit according to generally accepted government auditing standards and guidance from the Office of Management and Budget and the Government Accountability Office. KPMG is responsible for the attached management letter dated March 11, 2014, and the conclusion expressed in it.

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

Attachment

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

March 11, 2014

Office of Inspector General,
U.S. Department of Homeland Security, and
Chief Information Officer and Chief Financial Officer,
U.S. Department of Homeland Security United States Coast Guard

Ladies and Gentlemen:

We have audited the financial statements of the U.S. Department of Homeland Security (DHS or Department) for the year ended September 30, 2013 (referred to herein as the "fiscal year (FY) 2013 financial statements"), and have issued our report thereon dated December 11, 2013. In planning and performing our audit of the financial statements of DHS, in accordance with auditing standards generally accepted in the United States of America and *Government Auditing Standards*, we considered internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements. In conjunction with our audit of the financial statements, we also performed an audit of internal control over financial reporting in accordance with attestation standards issued by the American Institute of Certified Public Accountants.

In accordance with *Government Auditing Standards*, our *Independent Auditors' Report*, dated December 11, 2013, included internal control deficiencies identified during our audit 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 the U.S. Coast Guard (USCG or Coast Guard).

During our audit we noted certain matters involving internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management and communicated through Notices of Findings and Recommendations (NFRs), are intended to improve internal control or result in other operating efficiencies and are summarized as described below.

With respect to Coast Guard's financial systems' IT controls, we noted certain matters in the areas of security management, access controls, and configuration management. These matters are described in the *General IT Control Findings and Recommendations* section of this letter.

The Table of Contents identifies each section of the letter. We have provided a description of key Coast Guard financial systems and IT infrastructure within the scope of the FY 2013 DHS financial statement audit in Appendix A, and a listing of each IT NFR communicated to management during our audit in Appendix B.

During our audit we noted certain matters involving financial reporting internal controls (comments not related to IT) and other operational matters, including certain deficiencies in internal control that we consider to be significant deficiencies and material weaknesses, and communicated them in writing to management and those charged with governance in our *Independent Auditors' Report* and in a separate letter to the Office of Inspector General and the DHS Chief Financial Officer.

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements and on the effectiveness of internal control over financial reporting, and therefore may not bring to light all deficiencies in policies or procedures that may exist. We aim, however, to use our knowledge of DHS' organization gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time.

The purpose of this letter is solely to describe comments and recommendations intended to improve internal control or result in other operating efficiencies. Accordingly, this letter is not suitable for any other purpose.

Very truly yours,

KPMG LLP

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE, AND APPROACH

Objective

We have audited the financial statements of the U.S. Department of Homeland Security (DHS or Department) for the year ended September 30, 2013 (referred to herein as the "fiscal year (FY) 2013 financial statements"). In connection with our audit of the FY 2013 financial statements, we performed an evaluation of selected general information technology (IT) controls (GITCs) and IT application controls at the U.S. Coast Guard (USCG or Coast Guard) to assist in planning and performing our audit engagement.

Scope

The scope of our GITC and IT application control test work is described in Appendix A, which provides a description of the key Coast Guard financial systems and IT infrastructure within the scope of the Coast Guard component of the FY 2013 DHS consolidated financial statement audit.

Approach

General Information Technology Controls

The *Federal Information System Controls Audit Manual* (FISCAM), issued by the U.S. Government Accountability Office, formed the basis of our GITC evaluation procedures.

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 categories to be essential to the effective operation of GITCs and the IT environment:

- *Security Management* – Controls that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related security controls.

  - In conjunction with our test work of security management GITCs, limited after-hours physical security testing and social engineering at select Coast Guard facilities was conducted to identify potential control deficiencies in non-technical aspects of IT security.

- *Access Control* – Controls that limit or detect access to computer resources (data, programs, equipment, and facilities) and protect against unauthorized modification, loss, and disclosure.

- *Configuration Management* – Controls that help to prevent unauthorized changes to information system resources (software programs and hardware configurations) and provide reasonable assurance that systems are configured and operating securely and as intended.

- We performed technical information security testing for key Coast Guard network and system devices. The technical security testing was performed from within select DHS facilities and focused on production devices that directly support DHS' and Coast Guard's financial processing and key general support systems.

- *Segregation of Duties* – Controls that constitute policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations.

- *Contingency Planning* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

IT Application Controls

We performed testing over selected key IT application controls on financial systems and applications to assess the financial systems' internal controls over the input, processing, and output of financial data and transactions. FISCAM defines application controls as the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, or payroll.

SUMMARY OF FINDINGS

During FY 2012, Coast Guard took corrective action to address certain prior year IT control deficiencies. For example, Coast Guard made improvements over designing and implementing certain logical access, physical access, and configuration management controls, including controls relative to the scripting process, over Coast Guard information systems. However, during FY 2013, we continued to identify GITC deficiencies related to controls over security management (including deficiencies over physical security and security awareness), access control, and configuration management for Coast Guard core financial and feeder systems and associated General Support System environments.

Collectively, the 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 Coast Guard's internal controls over financial reporting and its operations. We consider these deficiencies, in aggregate, to contribute to the IT 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 Coast Guard contributes to the Department's non-compliance with the relevant federal financial management systems requirements of the *Federal Financial Management Improvement Act of 1996*.

Of the eight IT Notices of Findings and Recommendations (NFRs) issued during our FY 2013 testing, seven were repeat findings, either partially or in whole from the prior year, and one was a new finding. The eight IT NFRs issued represent deficiencies in three of the five FISCAM GITC categories.

The majority of findings resulted from the lack of properly documented, fully designed and implemented, adequately detailed, and consistently implemented financial system controls to comply with DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program,* requirements and National Institute of Standards and Technology guidance. Specifically, the findings stem from:

1. Inadequately designed and ineffective access control policies and procedures relating to the management of logical access to financial applications, databases, and support systems;
2. Insufficient logging of system events and monitoring of audit logs; and
3. Patch, configuration, and vulnerability management control deficiencies within systems.

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 Coast Guard financial data used by management and reported in Coast Guard's and DHS' 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 deficiencies identified.

GENERAL IT CONTROL FINDINGS AND RECOMMENDATIONS

Findings

During our audit of the FY 2013 DHS financial statements, we identified the following Coast Guard GITC deficiencies that, in the aggregate, contribute to the IT material weakness at the Department level.

<u>Security Management</u>

After-Hours Physical Security Testing

On June 20, July 15, July 18, and August 16, 2013, we performed after-hours physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects included physical access to printed or electronic media, equipment, or credentials residing within a Coast Guard employee's or contractor's work area or shared workspaces which could be used by others to gain unauthorized access to systems housing financial or other sensitive information. The testing was performed at various USCG locations in Baltimore, Maryland; Martinsburg, West Virginia (WV); Elizabeth City, North Carolina (NC); and Chesapeake, Virginia (VA) that process, maintain, and/or have access to financial data.

We observed 52 instances where passwords, keys, unsecured or unlocked credentials and external media, and printed materials marked "For Official Use Only" or containing sensitive Personally Identifiable Information were accessible by individuals without a "need to know".

Social Engineering

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 trickery or deception for the purpose of information gathering, or gaining computer system access.

On July 11, 2013, we performed social engineering testing from a DHS facility to identify risks related to Coast Guard personnel awareness of responsibilities for protecting sensitive IT information, including personal system access credentials, from disclosure to unauthorized personnel. We noted two instances where individuals divulged their Naval and Electronics Supply Support System (NESSS) application account password to KPMG auditors.

<u>Access Controls</u>

- Controls to notify Coast Guard system owners of separated or transferred military and civilian personnel and contractors and to generate reports of separated or transferred individuals to support periodic reviews of system access were not implemented.

- Controls to generate, and perform and document independent reviews of, required audit records of events on the Direct Access system were not implemented.

- Account management activities on Coast Guard financial systems (including Direct Access, Joint Uniform Military Pay System [JUMPS], and NESSS), including periodic recertification of access, were not consistently or timely documented or implemented in accordance with DHS and Coast Guard policy.

Configuration Management

- Password, security patch management, and configuration deficiencies were identified during the vulnerability assessment on hosts supporting USCG financial systems hosted at the Coast Guard Finance Center (FINCEN), Operations Systems Center (OSC), and Aviation Logistics Center (ALC).

Recommendations

We recommend that the Coast Guard Office of the Chief Information Officer (OCIO) and Office of the Chief Financial Officer (OCFO), in coordination with the DHS OCIO and the DHS OCFO**,** make the following improvements to Coast Guard's financial management systems and associated IT security program.

Security Management

- Continue to improve training with respect to IT security policies and procedures related to properly securing sensitive DHS and Coast Guard data within physical workspaces and protecting personal system access credentials from disclosure to unauthorized personnel, and perform periodic physical workspace audits and internal social engineering testing to re-enforce training principles.

Access Controls

- Complete efforts to document and implement enterprise-wide processes to ensure that system owners are notified and revoke access from separated or transferred military and civilian personnel and contractors timely in accordance with Coast Guard and DHS requirements.

- Implement monitoring controls over the Direct Access audit log generation and review process to ensure that logs are properly configured and secured from unauthorized modification, reviews are performed independently (with respect to segregation of duties principles) and evidence of audit log reviews is retained.

- Implement monitoring controls over the account management process to ensure that all users of Coast Guard systems are periodically revalidated in accordance with CBP and DHS requirements. If necessary and justified by operational and business requirements, ensure that documented requests for exceptions from DHS requirements for periodic account recertification follow established processes for DHS exceptions.

Configuration Management

- Implement the specific vendor-recommended corrective actions detailed in the NFRs that were issued for deficiencies identified during our vulnerability assessment.

IT APPLICATION CONTROLS

We conducted testing over certain Core Accounting System (CAS), Financial Procurement Desktop (FPD), JUMPS, Direct Access, NESSS, and Aviation Logistics Management Information System (ALMIS) application controls supporting in-scope processes during the Coast Guard component of the FY 2013 DHS financial statement audit and did not identify any control deficiencies.

Appendix A

Description of Key Coast Guard Financial Systems and IT Infrastructure within the Scope of the FY 2013 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 Coast Guard component of the DHS FY 2013 financial statement 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 FINCEN in VA. CAS interfaces with FPD, also located at FINCEN. CAS is used by financial management individuals as CAS is the main system of record for financial information. CAS has a Hewlett-Packard (HP) UNIX operating system with an Oracle database, and the organizations responsible for CAS are FINCEN, Coast Guard OCFO, and Coast Guard OCIO.

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, and has an HP UNIX operating system and Oracle database. The organizations responsible for CAS are FINCEN, Coast Guard OCFO, and Coast Guard OCIO.

Joint Uniform Military Pay System (JUMPS)

JUMPS is an IBM zOS mainframe application and database that is used for paying USCG active and reserve payroll and is mainly used by Pay and Personnel Center (PPC) employees. JUMPS is located at the Burlington Northern Santa Fe data center in Kansas. The responsible organization for JUMPS is PPC, which falls under the purview of the Coast Guard OCIO.

Direct Access

Direct Access is the system of record for all functionality, data entry, and processing of payroll events for the Coast Guard. Every Coast Guard employee is a user of the system. Employees may use Direct Access to correct their own personal information, such as address and beneficiaries. The main financial users use Direct Access to process payroll events and change personnel records such as pay scales. Up until June 2013, Direct Access was maintained by IBM Application On Demand (IBM AOD) in the iStructure data center facility in Arizona (AZ) with an automated backup site located in a Qwest data center in VA. Starting in June 2013, Direct Access is maintained by Addx Corporation and is located in VA. Direct Access is a PeopleSoft application residing on servers operating the Solaris and Windows Server 2000 operating systems and is supported by an Oracle database. The responsible organization for Direct Access is the Coast Guard OCIO.

Global Pay (Direct Access II)

Global Pay provides retiree and annuitant support services. Until June 2013, Global Pay was maintained by IBM AOD in the iStructure data center facility in AZ with an automated backup site located in a

Qwest data center in VA. Starting in June 2013, Global Pay is maintained by Addx Corporation and is located in VA. Global Pay is a PeopleSoft application residing on servers operating the IBM xSeries operating system and is supported by an Oracle database. The responsible organization for Global Pay is the Coast Guard OCIO.

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. NESSS is used by both financial and logistics personnel across numerous Coast Guard locations. NESSS is located at the OSC in WV, resides on servers operating the Microsoft Windows 2003 and HP/UNIX operating systems, and is supported by an Oracle database. The responsible organizations for NESSS are the Office of Logistics Program Management and OSC, which act under the purview of the Coast Guard OCIO.

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, 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 NC hosts the ALMIS application. ALMIS is used by both financial and logistics personnel across numerous Coast Guard locations. ALMIS is located at the ALC in NC and has a HP UNIX operating system and a Haley database. The responsible organization for ALMIS is ALC.

Appendix B

FY 2013 IT Notices of Findings and Recommendations at Coast Guard

FY 2013 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CG-IT-13-01	Lack of Consistent Contractor, Civilian, and Military Account Termination Notification Process for Coast Guard Systems	Access Controls		X
CG-IT-13-02	Weakness in Direct Access Audit Logs and Segregation of Duties	Access Controls		X
CG-IT-13-03	Weakness in Direct Access Annual User Recertification	Access Controls		X
CG-IT-13-04	Security Awareness Issues Identified During Social Engineering Testing at Surface Forces Logistics Center	Security Management		X
CG-IT-13-05	Security Awareness Issues Identified during After-Hours Physical Security Testing at the Surface Forces Logistics Center, OSC, ALC, and FINCEN	Security Management		X
CG-IT-13-06	Access and Configuration Management Controls - Vulnerability Assessment	Configuration Management		X
CG-IT-13-07	Weakness in JUMPS Annual User Recertification	Access Controls	X	
CG-IT-13-08	Weakness in NESSS Annual User Recertification	Access Controls		X

Appendix A
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary for Management
Chief Financial Officer
Chief Information Officer
Chief Information Security Officer
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@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:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Office of Investigations Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

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