

**Information Technology
Management Letter for the
Office of Financial
Management and Office of
Chief Information Officer
Components of the FY 2014
Department of Homeland
Security Financial Statement
Audit**





HIGHLIGHTS

Information Technology Management Letter for the Office of Financial Management and Office of Chief Information Officer Components of the FY 2014 Department of Homeland Security Financial Statement Audit

April 14, 2015

Why We Did This

Each year, our independent auditors identify component-level information technology control deficiencies as part of the DHS consolidated financial statement audit. This letter provides details that were not included in the fiscal year (FY) 2014 DHS Agency Financial Report.

What We Recommend

We recommend the Chief Information Officer and Chief Financial Officer make improvements to DHS' financial management systems and associated information technology security program.

For Further Information:

Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-IG.OfficePublicAffairs@oig.dhs.gov

What We Found

We contracted with the independent public accounting firm KPMG, LLP to perform the audit of the consolidated financial statements of the U.S. Department of Homeland Security (DHS) for the year ended September 30, 2014. KPMG, LLP evaluated selected general information technology controls and business process application controls at DHS' Office of Financial Management and Office of Chief Information Officer. KPMG, LLP continued to identify deficiencies related to access controls and vulnerability management controls of DHS' core financial system. Inadequate protection of DHS information systems and data from those without a need to know or a need for access puts DHS' sensitive electronic and physical data at risk of loss, theft, or misuse.



OFFICE OF INSPECTOR GENERAL

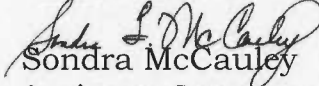
Department of Homeland Security

Washington, DC

April 14, 2015

TO: Luke McCormack
Chief Information Officer

Chip Fulghum
Chief Financial Officer

FROM: 
Sondra McCauley
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the Office of Financial Management and Office of Chief Information Officer Components of the FY 2014 Department of Homeland Security Financial Statement Audit*

Attached for your information is our final report, *Information Technology Management Letter for the Office of Financial Management and Office of Chief Information Officer Components of the FY 2014 Department of Homeland Security's Financial Statement Audit*. This report contains comments and recommendations related to information technology internal control deficiencies. The observations did not meet the criteria to be reported in the *Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting*, dated November 14, 2014, which was included in the FY 2014 DHS Agency Financial Report.

The independent public accounting firm KPMG, LLP conducted the audit of DHS' FY 2014 financial statements and is responsible for the attached information technology management letter and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control, nor do we provide conclusions on compliance with laws and regulations. We will post the final report on our website.

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

Attachment



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

December 19, 2014

Office of Inspector General,
Chief Information Officer, and Chief Financial Officer,
U.S. Department of Homeland Security,
Washington, DC

Ladies and Gentlemen:

In planning and performing our audit of the consolidated financial statements of the U.S. Department of Homeland Security (DHS or Department), as of and for the year ended September 30, 2014 (hereinafter, referred to as the “fiscal year (FY) 2014 DHS consolidated financial statements”), in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States; and Office of Management and Budget Bulletin No. 14-02, *Audit Requirements for Federal Financial Statements*, 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 consolidated 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.

During our audit we noted certain matters involving internal control and other operational matters at the DHS Office of Financial Management (OFM) and the DHS Office of Chief Information Officer (OCIO), components of DHS that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies.

With respect to financial systems, we noted certain internal control deficiencies at OFM and OCIO in the general IT control areas of access controls and configuration management. These matters are described in the *Findings and Recommendations* section of this letter.

Additionally, at the request of the DHS Office of Inspector General (OIG), we performed additional non-technical information security procedures to identify instances where OFM personnel did not adequately comply with requirements for safeguarding sensitive material or assets from unauthorized access or disclosure. These matters are described in the *Observations Related to Non-Technical Information Security* section of this letter.

We have provided a description of the key DHS financial system and IT infrastructure within the scope of the FY 2014 DHS financial statement audit in Appendix A, and a listing of each OFM



and OCIO IT Notice of Finding and Recommendation 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 at OFM, and communicated them in writing to management and those charged with governance in our *Independent Auditors' Report* and in a separate letter to the OIG and the DHS Chief Financial Officer.

Our audit procedures are designed primarily to enable us to form opinions on the FY 2014 DHS consolidated 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

Department of Homeland Security
Information Technology Management Letter
Office of Financial Management / Office of Chief Information Officer
September 30, 2014

TABLE OF CONTENTS

	Page
Objective, Scope, and Approach	2
Summary of Findings	4
Findings and Recommendations	5
Findings	5
Recommendations	5
Observations Related to Non-Technical Information Security	6

APPENDICES

Appendix	Subject	Page
A	Description of Key OFM/OCIO Financial Systems and IT Infrastructure within the Scope of the FY 2014 DHS Financial Statement Audit	8
B	FY 2014 IT Notices of Findings and Recommendations at OFM/OCIO	10

OBJECTIVE, SCOPE, AND APPROACH

Objective

We audited the consolidated financial statements of the U.S. Department of Homeland Security (DHS or Department) for the year ended September 30, 2014 (hereinafter, referred to as the “fiscal year (FY) 2014 DHS consolidated financial statements”). In connection with our audit of the FY 2014 DHS consolidated financial statements, we performed an evaluation of selected general information technology (IT) controls (GITCs) and business process application controls (BPACs) at the DHS Office of Financial Management (OFM) and the DHS Office of Chief Information Officer (OCIO), components of DHS, to assist in planning and performing our audit engagement. At the request of the DHS Office of Inspector General (OIG), we also performed additional information security testing procedures to assess certain non-technical areas related to the protection of sensitive IT and financial information and assets.

Scope and Approach

General Information Technology Controls

The *Federal Information System Controls Audit Manual* (FISCAM), issued by the U.S. Government Accountability Office (GAO), 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 as essential to the effective operation of GITCs and the IT environment:

1. *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.
2. *Access Control* – Controls that limit or detect access to computer resources (data, programs, equipment, and facilities) and protect against unauthorized modification, loss, and disclosure.
3. *Configuration Management* – Controls that help 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.
4. *Segregation of Duties* – Controls that constitute policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations.
5. *Contingency Planning* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

Department of Homeland Security
Information Technology Management Letter
Office of Financial Management / Office of Chief Information Officer
September 30, 2014

While each of these five FISCAM categories were considered during the planning and risk assessment phase of our audit, we selected GITCs for evaluation based on their relationship to the ongoing effectiveness of process-level automated controls or manual controls with one or more automated components. This includes those controls which depend on the completeness, accuracy, and integrity of information provided by the entity in support of our financial audit procedures. Consequently, FY 2014 GITC procedures at OFM/OCIO did not necessarily represent controls from each FISCAM category.

Business Process Application Controls

Where relevant GITCs were determined to be operating effectively, we performed testing of selected BPACs (process-level controls which were either fully automated or manual with an automated component) supporting financial systems and applications to assess the financial systems' internal controls over the input, processing, and output of financial data and transactions.

FISCAM defines BPACs as the automated and/or manual controls applied to business transaction flows and related to the completeness, accuracy, validity, and confidentiality of transactions and data during application processing. They typically cover the structure, policies, and procedures that operate at a detailed business process (cycle or transaction) level and operate over individual transactions or activities across business processes.

Financial System Functionality

In recent years, we have noted that limitations in DHS financial systems functionality may be inhibiting the agency's ability to implement and maintain internal controls, including effective GITCs and BPACs supporting financial data processing and reporting. Many key financial and feeder systems have not been substantially updated since being inherited from legacy agencies several years ago. Therefore, in FY 2014, we continued to evaluate and consider the impact of financial system functionality on internal control over financial reporting.

Non-Technical Information Security Testing

To complement our IT controls test work, we conducted limited after-hours physical security testing and social engineering at selected DHS facilities to identify potential weaknesses in non-technical aspects of IT security. This includes those related to OFM personnel awareness of policies, procedures, and other requirements governing the protection of sensitive IT and financial information and assets from unauthorized access or disclosure. This testing was performed in accordance with the FY 2014 DHS *Security Testing Authorization Letter* (STAL) signed by KPMG, DHS OIG, and DHS management.

Appendix A provides a description of the key OFM financial system and IT infrastructure within the scope of the FY 2014 DHS financial statement audit.

SUMMARY OF FINDINGS

During FY 2014, we continued to identify GITC deficiencies at OFM/OCIO related to controls over physical access to DHS' core financial system. We also identified deficiencies related to vulnerability management controls that had not been reviewed in prior years.

The conditions supporting our findings collectively limited DHS' ability to ensure that critical financial and operational data were maintained in such a manner as to ensure confidentiality, integrity, and availability. Of the three IT Notices of Findings and Recommendations (NFRs) issued during our FY 2014 testing at OFM/OCIO, two were repeat findings, either partially or in whole from the prior year, and one was a new finding. The three IT NFRs issued represent deficiencies and observations related to three of the five FISCAM GITC categories.

The majority of findings resulted from a lack of properly documented, fully designed and implemented, adequately detailed, and consistently implemented financial system controls to comply with the requirements of DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program*, National Institute of Standards and Technology guidance, and OFM and OCIO policies and procedures, as applicable. The most significant weaknesses from a financial statement audit perspective continued to include:

1. Inadequately monitored physical access to system components for DHS' core financial system; and
2. Configuration management controls that were not fully effective.

While the recommendations made by us should be considered by DHS, it is ultimately the responsibility of DHS management to determine the most appropriate method(s) for addressing the deficiencies identified.

FINDINGS AND RECOMMENDATIONS

Findings

During our audit of the FY 2014 DHS consolidated financial statements, we identified the following GITC deficiencies at OFM/OCIO:

Access Controls

- Responsibilities related to the performance of periodic reviews of physical access to the interior rooms within DHS Enterprise Data Center DC-1 hosting DHS' core financial system were not fully defined or implemented.

Configuration Management

- Security patch management and configuration deficiencies were identified during vulnerability assessments of system components supporting DHS' core financial system.

Recommendations

We recommend that the Office of Chief Financial Officer (OCFO) and DHS OCIO make the following improvements to DHS' financial management system and associated IT security program (in accordance with DHS requirements, as applicable):

Access Controls

- Fully define and document responsibility for controls related to periodic review of physical access privileges for the interior rooms of DHS Enterprise Data Center DC-1 hosting DHS' core financial system, including developing and implementing revised agreements with business partners and third-party service organizations, as appropriate.

Configuration Management

- Implement specific vendor-recommended corrective actions detailed in the NFR issued for deficiencies identified during the vulnerability assessment.

OBSERVATIONS RELATED TO NON-TECHNICAL INFORMATION SECURITY

To complement our IT controls test work during the FY 2014 audit, we performed additional non-technical information security procedures at DHS. These procedures included after-hours physical security walkthroughs and social engineering to identify instances where OFM personnel did not adequately comply with requirements for safeguarding sensitive material or assets from unauthorized access or disclosure. These procedures were performed in accordance with the FY 2014 STAL, signed by DHS OIG management, KPMG management, and DHS management (Chief Information Officer [CIO], Chief Information Security Officer, Chief Financial Officer, Chief Privacy Officer, and Chief Security Officer) on June 3, 2014, and transmitted to the DHS CIO Council on June 12, 2014.

Social Engineering

Social engineering is defined as the act of manipulating people into performing actions or divulging sensitive information. The term typically applies to trickery or deception for the purpose of information gathering or obtaining computer system access. The objective of our social engineering tests was to identify the extent to which OFM personnel were willing to divulge network or system passwords that, if exploited, could compromise DHS sensitive information.

To conduct this testing, we made phone calls from various OFM locations at various times throughout the audit. Posing as DHS technical support personnel, we attempted to solicit access credentials from OFM users. Attempts to log into DHS systems were not performed; however, we assumed that disclosed passwords that met the minimum password standards established by DHS policy were valid exceptions. During social engineering performed at OFM, we attempted to call a total of 45 employees and contractors and reached 8. Of those 8 individuals with whom we spoke, no individuals divulged their passwords in violation of DHS policy.

The selection of attempted or connected calls was not statistically derived; therefore, the results described here should not be used to extrapolate to OFM as a whole.

After-Hours Physical Security Walkthroughs

Multiple DHS policies, including the DHS Sensitive Systems Policy Directive 4300A, the DHS Privacy Office *Handbook for Safeguarding Sensitive Personally-Identifiable Information (PII)*, and DHS Management Directive 11042.1, *Safeguarding Sensitive but Unclassified (FOUO) Information*, mandate the physical safeguarding of certain materials and assets which, if compromised either due to external or insider threat, could result in unauthorized access, disclosure, or exploitation of sensitive IT or financial information.

We performed procedures to determine whether OFM personnel consistently exercised responsibilities related to safeguarding sensitive materials as defined in these policies. Specifically, we performed escorted walkthroughs of workspaces – including cubicles, offices, shared workspaces, and/or common areas (e.g., areas where printers were hosted) – at OFM facilities that processed, maintained, and/or had access to financial data during FY 2014. We inspected workspaces to identify instances where materials

Department of Homeland Security
Information Technology Management Letter
Office of Financial Management / Office of Chief Information Officer
September 30, 2014

designated by DHS policy as requiring physical security from unauthorized access were left unattended. Exceptions noted were validated by designated representatives from the OIG and OCIO.

During after-hours physical security walkthroughs performed at OFM, we inspected a total of 53 workspaces. Of those, five were observed to have material – including, but not limited to, information marked “FOUO” and documents containing sensitive PII – left unattended and unsecured after business hours in violation of DHS policy.

The selection of inspected areas was not statistically derived; therefore, the results described here should not be used to extrapolate to OFM as a whole.

Appendix A

Description of Key OFM/OCIO Financial System and IT Infrastructure within the Scope of the FY 2014 DHS Financial Statement Audit

Department of Homeland Security
Information Technology Management Letter
Office of Financial Management / Office of Chief Information Officer
September 30, 2014

Below is a description of the significant OFM/OCIO financial management system and supporting IT infrastructure included in the scope of the FY 2014 DHS financial statement audit.

DHS Treasury Information Executive Repository (DHSTIER)

DHSTIER is the system of record for DHS' consolidated financial statements and is used to track, process, and perform validation and edit checks against monthly financial data uploaded from each DHS component's core financial management systems. DHSTIER is administered jointly by the OCFO Resource Management Transformation Office and the OCFO Office of Financial Management.

Appendix B
FY 2014 IT Notices of Findings and Recommendations at
OFM/OCIO

Department of Homeland Security
Information Technology Management Letter
Office of Financial Management / Office of Chief Information Officer
 September 30, 2014

FY 2014 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
CONS-IT-14-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at OFM	Security Management		X
CONS-IT-14-02	Weaknesses Identified during the Vulnerability Assessment on DHSTIER	Configuration Management	X	
CONS-IT-14-03	Lack of Documented Agreement between DHS and the National Aeronautics and Space Administration (NASA) for Assignment of Control Responsibility for Physical Access Controls over the DHSTIER System Environment	Access Controls		X

ADDITIONAL INFORMATION AND COPIES

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 Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.



OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

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