

**Information Technology
Management Letter for
the Office of Financial
Management and Office
of the Chief Information
Officer Components of
the FY 2016 Department
of Homeland Security
Financial Statement
Audit**





DHS OIG HIGHLIGHTS

Information Technology Management Letter for the Office of Financial Management and Office of the Chief Information Officer Components of the FY 2016 Department of Homeland Security Financial Statement Audit

June 28, 2017

Why We Did This Audit

Each year, our independent auditors identify component-level information technology (IT) control deficiencies as part of the DHS consolidated financial statement audit. This letter provides details that were not included in the fiscal year (FY) 2016 DHS Agency Financial Report.

What We Recommend

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

For Further Information:

Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.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, 2016. KPMG evaluated selected general IT controls and business process application controls at the Office of Financial Management (OFM) and Office of the Chief Information Officer (OCIO). KPMG identified deficiencies related to access controls and configuration management of OFM's and OCIO's core financial and feeder systems.

The deficiencies collectively limited OFM and OCIO's ability to ensure that critical financial and operational data were maintained in such a manner as to ensure their confidentiality, integrity, and availability. In addition, certain of these deficiencies adversely impacted internal controls over DHS' financial reporting and its operation and therefore are considered to collectively represent a material weakness reported in the FY 2016 DHS Agency Financial Report.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

June 28, 2017

MEMORANDUM FOR: Richard Staropoli
Chief Information Officer

Stacy Marcott
Acting 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 the Chief
Information Officer Components of the FY 2016
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 the Chief Information Officer Components of the FY 2016 Department of Homeland Security Financial Statement Audit*. This report contains comments and recommendations related to information technology internal control deficiencies. The deficiencies did not meet the criteria to be reported in the *Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting*, dated November 14, 2016, which was included in the FY 2016 DHS Agency Financial Report.

The independent public accounting firm KPMG LLP conducted the audit of DHS' FY 2016 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 Kevin Burke, Acting Director, Information Systems and Acquisitions Division, at (202) 254-5450.

Attachment



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

December 15, 2016

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

Ladies and Gentlemen:

We planned and performed 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, 2016, 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. 15-02, *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 DHS Office of the Chief Information Officer (OCIO) 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.

We also noted certain internal control deficiencies at OFM and OCIO during our audit that, in aggregate and when combined with certain internal control deficiencies identified at certain other DHS components, contributed to a material weakness in information technology (IT) controls and financial system functionality at the DHS Department-wide level. Specifically, with respect to financial systems at DHS, we noted certain matters in the general IT control areas of access controls, security management, 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 in which OFM and OCIO 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 Fiscal Year (FY) 2016 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 OCIO, including certain deficiencies in internal control that we consider to be 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 OIG and the DHS Chief Financial Officer.

Our audit procedures are designed primarily to enable us to form opinions on the FY 2016 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 OFM's and OCIO's organization gained during our work to make comments and suggestions that we hope will be useful.

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 the Chief Information Officer
September 30, 2016

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 and OCIO Financial Systems and IT Infrastructure within the Scope of the FY 2016 DHS Financial Statement Audit | 7 |
| B | FY 2016 IT Notices of Findings and Recommendations at OFM and OCIO | 9 |

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, 2016, (hereinafter, referred to as the “Fiscal Year (FY) 2016 DHS consolidated financial statements”). In connection with our audit of the FY 2016 DHS consolidated financial statements, we performed an evaluation of selected general information technology (IT) controls (GITC) and IT application controls at the Office of Financial Management (OFM) and the Office of the Chief Information Officer (OCIO), 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 U.S. Government Accountability Office (GAO) issued the *Federal Information System Controls Audit Manual* (FISCAM), which formed the basis for 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. It 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:

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.

Although each of these FISCAM categories was considered during the planning and risk assessment phase of our audit, we selected GITCs and IT ELCs 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 that depend on the completeness, accuracy, and integrity of information provided by the entity in support of our financial audit procedures. Consequently,

Department of Homeland Security
Information Technology Management Letter
Office of Financial Management / Office of the Chief Information Officer
September 30, 2016

FY 2016 GITC procedures evaluated at OFM and OCIO did not necessarily represent controls from each FISCAM category.

Business Process Application Controls

Where relevant GITCs were operating effectively, we tested selected IT application controls (process-level controls — fully automated or manual with an automated component) on financial systems and applications to assess internal controls over the input, processing, and output of financial data and transactions.

FISCAM defines Business Process Application Controls (BPAC) 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. BPACs 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 OFM and OCIO financial systems' functionality may be inhibiting the agency's ability to implement and maintain internal controls, including effective GITCs and IT application controls supporting financial data processing and reporting. Many key financial feeder systems are not fully integrated with the main financial system. Therefore, in FY 2016, 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 OFM and OCIO component facilities to identify potential weaknesses in non-technical aspects of IT security. This includes those related to component 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 2016 DHS *Security Testing Authorization Letter* (STAL) signed by KPMG LLP, DHS OIG, and DHS management.

Appendix A provides a description of the key OFM and OCIO financial systems and IT infrastructure within the scope of the FY 2016 DHS financial statement audit.

SUMMARY OF FINDINGS

During our FY 2016 assessment of GITCs and application controls, we identified GITC deficiencies related to access controls and configuration management of OFM and OCIO's core financial and feeder systems. In many cases, new control deficiencies reflected weaknesses that were historically operating effectively in prior years.

The conditions supporting our findings collectively limited OFM and OCIO's ability to ensure that critical financial and operational data were maintained in such a manner as to ensure their confidentiality, integrity, and availability. In addition, certain of these deficiencies at OFM and OCIO adversely impacted the internal controls over DHS' financial reporting and its operation and we consider them to collectively contribute to a Department-wide material weakness regarding IT controls and financial system functionality for DHS, under standards established by the American Institute of Certified Public Accountants and the U.S. GAO.

Of the three IT Notices of Findings and Recommendations (NFR) issued during our FY 2016 testing at OFM and OCIO, one was a repeat finding, either wholly or in part from the prior year, and two were new findings. The three IT NFRs issued represent deficiencies and observations related to three of the five FISCAM GITC categories.

The majority of the deficiencies that our audit identified were related to noncompliance with financial system controls. According to DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program*; National Institute of Standards and Technology guidance; and DHS policies, financial system controls lacked proper documentation, were not fully designed and implemented, were inadequately detailed, and were inconsistently implemented.

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

FINDINGS AND RECOMMENDATIONS

Findings

During our audit of the FY 2016 DHS consolidated financial statements, we identified the following GITC deficiencies at OFM and OCIO:

Access Controls

- Policy and procedures did not appropriately document password configurations in accordance with Department-wide policy.

Configuration Management

- The Configuration Management Plan was in draft and not finalized for the majority of FY 2016.

Recommendations

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

Access Controls

- Implement changes to password configurations to ensure compliance with Department policy.

Configuration Management

- Finalize the Configuration Management Plan.

OBSERVATIONS RELATED TO NON-TECHNICAL INFORMATION SECURITY

To complement our IT controls test work during the FY 2016 audit, we performed additional non-technical information security procedures at OFM and OCIO. These procedures included after-hours physical security walkthroughs to identify instances in which OFM and OCIO 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 2016 *Security Testing Authorization Letter* (STAL) signed by DHS OIG management, KPMG management, and DHS management.

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 (MD) 11042.1, *Safeguarding Sensitive but Unclassified (SBU) (FOUO) Information*, mandate the physical safeguarding of certain materials and assets that, 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 and OCIO 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 and OCIO facilities that processed, maintained, and/or had access to financial data during FY 2016. We inspected workspaces to identify instances where materials designated by DHS policy as requiring physical security from unauthorized access were left unattended. Exceptions noted were validated by designated representatives from DHS OFM, DHS OIG, and DHS OCIO.

During after-hours physical security walkthroughs performed at DHS, we inspected a total of 69 workspaces. Of those, 3 were observed to have material – including, but not limited to, system passwords, information marked “FOUO” or otherwise meeting the criteria established by DHS MD 11042.1, documents containing sensitive PII, and government-issued laptops, mobile devices, or storage media – 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 and OCIO as a whole.

Appendix A

**Description of Key OFM and OCIO Financial Systems and IT Infrastructure within the Scope of the
FY 2016 DHS Financial Statement Audit**

Department of Homeland Security
Information Technology Management Letter
Financial Management Division / Office of Chief Information Officer
September 30, 2016

Below is a description of the significant OFM and OCIO financial management system and supporting IT infrastructure included in the scope of the FY 2016 DHS financial statement audit.

DHS Treasury Information Executive Repository (DHSTIER)

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

Procurement Request Information System (PRISM)

PRISM is a major application that the DHS Office of the Chief Procurement Officer (OCPO) hosts. PRISM provides comprehensive, Federal Acquisition Regulations (FAR)-based acquisition support for multiple DHS entities.

An Oracle database with UNIX-based servers supports PRISM, and the system resides in Datacenter 1 in Stennis, MS.

Department of Homeland Security
Information Technology Management Letter
Financial Management Division / Office of Chief Information Officer
September 30, 2016

Appendix B

FY 2016 IT Notices of Findings and Recommendations at OFM and OCIO

Department of Homeland Security
Information Technology Management Letter
 Financial Management Division / Office of Chief Information Officer
 September 30, 2016

Office of Financial Management (OFM) / Office of the Chief Information Officer (OCIO)

| FY 2016 NFR # | NFR Title | FISCAM Control Area | New Issue | Repeat Issue |
|----------------------|--|----------------------------|------------------|---------------------|
| CONS-IT-16-01 | Security Awareness Issues Identified during After-Hours Physical Security Testing at DHS Consolidated | Security Management | | X |
| CONS-IT-16-02 | Weaknesses with DHS Treasury Information Executive Repository (DHSTIER) Baseline Configuration Policy and Procedures | Access Controls | X | |
| CONS-IT-16-03 | Weaknesses with Procurement Request Information System Management (PRISM) Configuration Management Policy and Procedures | Configuration Management | X | |



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
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 Privacy Officer

Management Directorate

Deputy Under Secretary
Acting Chief Financial Officer
Chief Information Officer
Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

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