

**Information Technology  
Management Letter for the  
Office of Financial  
Management and Office of  
Chief Information Officer  
Components of the FY 2015  
Department of Homeland  
Security Financial Statement  
Audit**





# DHS OIG HIGHLIGHTS

## *Information Technology Management Letter for the Office of Financial Management and Office of Chief Information Officer Components of the FY 2015 Department of Homeland Security Financial Statement Audit*

---

**May 6, 2016**

### **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 2015 DHS Agency Financial Report.

### **What We Recommend**

We recommend that OFM, in coordination with the DHS Chief Information Officer and Chief Financial Officer, make improvements to its 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-OIG.OfficePublicAffairs@oig.dhs.gov](mailto: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, 2015. KPMG, LLP performed after hours physical security walkthroughs and social engineering to identify instances where DHS OFM and DHS Office of the Chief Information Officer personnel did not comply with requirements for safeguarding sensitive assets from unauthorized access or disclosure. KPMG, LLP attempted to call a total of 28 employees and contractors and reached 8. Of the 8 contacted, none divulged passwords in violation of DHS policy.



## OFFICE OF INSPECTOR GENERAL

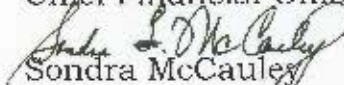
Department of Homeland Security

Washington, DC 20528 / [www.oig.dhs.gov](http://www.oig.dhs.gov)

May 6, 2016

MEMORANDUM FOR: Luke McCormack  
Chief Information Officer

The Honorable Chip Fulghum  
Deputy Under Secretary for Management  
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 2015 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 2015 Department of Homeland Security 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 2015 Financial Statements and Internal Control over Financial Reporting*, dated November 13, 2015, which was included in the FY 2015 DHS Agency Financial Report.

The independent public accounting firm KPMG, LLP conducted the audit of DHS' FY 2015 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 and Acquisitions Division, at (202) 254-5451.

Attachment



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

December 20, 2015

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, 2015 (hereinafter, referred to as the “fiscal year (FY) 2015 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. 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.

At the request of the DHS Office of Inspector General (OIG), we performed non-technical information security procedures to identify instances where DHS Office of Financial Management (OFM) and DHS Office of Chief Information Officer (OCIO) personnel did not comply with requirements for safeguarding sensitive material or assets from unauthorized access or disclosure. These matters are described in this letter.

During our audit, we noted certain matters involving financial reporting internal controls (comments not related to information technology) 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 2015 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, 2015

---

## **OBJECTIVE**

We audited the consolidated financial statements of the U.S. Department of Homeland Security (DHS or Department) for the year ended September 30, 2015 (hereinafter, referred to as the “fiscal year (FY) 2015 DHS consolidated financial statements”). In connection with our audit of the FY 2015 DHS consolidated financial statements, at the request of the DHS Office of Inspector General (OIG), we performed information security testing procedures at the Office of Financial Management (OFM) and the Office of Chief Information Officer (OCIO), components of DHS, to assess certain non-technical areas related to the protection of sensitive information technology (IT) and financial information and assets.

Specifically, we performed after-hours physical security walkthroughs and social engineering to identify instances where DHS OFM and DHS OCIO personnel did not comply with requirements for safeguarding sensitive material or assets from unauthorized access or disclosure. These procedures were performed in accordance with the FY 2015 *Security Testing Authorization Letter* (STAL), signed by DHS OIG management, KPMG management, and DHS management on May 20, 2015, and transmitted to the DHS CIO Council on May 27, 2015.

## **SUMMARY OF FINDINGS**

### **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 gathering information 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 28 employees and contractors and reached 8. Of the 8 individuals with whom we spoke, none divulged 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 (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.

Department of Homeland Security  
*Information Technology Management Letter*  
*Office of Financial Management / Office of Chief Information Officer*  
September 30, 2015

---

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 2015. 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 the OIG and OCIO.

During after-hours physical security walkthroughs performed at OFM, we inspected a total of 68 workspaces. Of those, six were observed to have material – including information marked “FOUO” – 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.

**FY 2015 IT NOTICES OF FINDINGS AND RECOMMENDATIONS AT DHS MANAGEMENT  
DIRECTORATE**

<b>FY 2015 NFR #</b>	<b>NFR Title</b>	<b>FISCAM Control Area</b>	<b>New Issue</b>	<b>Repeat Issue</b>
CONS-IT-15-01	Security Awareness Issues Identified during After-Hours Physical Security Testing at OFM	Security Management		X



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

---

**Appendix E**  
**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

**Office of Financial Management**

Deputy Under Secretary  
Chief Financial Officer  
Chief Information Officer

**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](http://www.oig.dhs.gov).

For further information or questions, please contact Office of Inspector General Public Affairs at: [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto: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](http://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