

OFFICE OF INSPECTOR GENERAL

**Information Technology
Management Letter for the
United States Secret Service
Component of the FY 2015
Department of Homeland Security
Financial Statement Audit**



Homeland
Security

**May 2, 2016
OIG-16-69**



DHS OIG HIGHLIGHTS

Information Technology Management Letter for the United States Secret Service Component of the FY 2015 Department of Homeland Security Financial Statement Audit

May 2, 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 (FY) 2015 DHS Agency Financial Report.

What We Recommend

We recommend that USSS, in coordination with the DHS Chief Information Officer and Chief Financial Officer, make improvements to its financial 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

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 for the year ended September 30, 2015. KPMG, LLP evaluated selected general IT controls and business process application controls at the United States Secret Service (USSS). KPMG, LLP determined that USSS took corrective action to address one prior-year IT control deficiency.

However, KPMG continued to identify general IT control deficiencies related to access controls for USSS. The conditions supporting our findings collectively limited USSS' ability to ensure that critical financial and operational data were maintained in such a manner as to ensure confidentiality, integrity, and availability.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

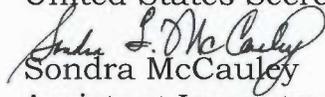
Washington, DC 20528 / www.oig.dhs.gov

May 2, 2016

MEMORANDUM FOR: Kevin Nally
Chief Information Officer
United States Secret Service

Gwendolyn Sykes
Chief Financial Officer
United States Secret Service

FROM:


Sondra McCauley
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the
United States Secret Service Component 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 United States Secret Service Component 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,
U.S. Department of Homeland Security, and
Chief Information Officer and Chief Financial Officer,
U.S. Secret Service,
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.

During our audit we noted certain matters involving internal control and other operational matters at the United States Secret Service (USSS), a component 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 at the USSS, we noted certain internal control deficiencies in the general information technology (IT) control area of access controls. 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 USSS 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 USSS financial system and IT infrastructure within the scope of the FY 2015 DHS financial statement audit in Appendix A, and a listing of each



USSS 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 USSS, 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 USSS 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
U.S. Secret Service
September 30, 2015

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 USSS Financial Systems and IT Infrastructure within the Scope of the FY 2015 DHS Financial Statement Audit | 7 |
| B | FY 2015 IT Notices of Findings and Recommendations at USSS | 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, 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, we performed an evaluation of selected general information technology (IT) controls (GITCs), and IT application controls at the United States Secret Service (USSS), a component 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 and IT Entity-Level Controls

The *Federal Information System Controls Audit Manual* (FISCAM), issued by the U.S. Government Accountability Office (GAO), 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. 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:

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.

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

Department of Homeland Security
Information Technology Management Letter
U.S. Secret Service
September 30, 2015

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, FY 2015 GITC procedures at USSS 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 over selected BPACs (process-level controls that were either fully automated or manual with an automated component) 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 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.

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 USSS facilities to identify potential weaknesses in non-technical aspects of IT security. This includes USSS 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 2015 DHS *Security Testing Authorization Letter* (STAL) signed by KPMG, DHS OIG, and DHS management.

Appendix A provides a description of the key USSS financial systems and IT infrastructure within the scope of the FY 2015 DHS financial statement audit.

Department of Homeland Security
Information Technology Management Letter
U.S. Secret Service
September 30, 2015

SUMMARY OF FINDINGS

During FY 2015, we identified GITC deficiencies at USSS related to access controls.

The conditions supporting our findings collectively limited USSS' ability to ensure that critical financial and operational data were maintained in such a manner as to ensure confidentiality, integrity, and availability.

Of the two IT notices of findings and recommendations (NFRs) issued during our FY 2015 testing at USSS, one was a repeat finding, either partially or in whole from the prior year, and one was a new finding. The two IT NFRs issued represent deficiencies and observations related to two 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 the requirements of DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program*; National Institute of Standards and Technology guidance; and USSS policies and procedures, as applicable. The most significant weakness from a financial statement audit perspective included:

- Lack of a process and documentation surrounding account management.

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

FINDINGS AND RECOMMENDATIONS

Findings

During our audit of the FY 2015 DHS consolidated financial statements, we identified the following GITC deficiencies at USSS:

Access Controls

- Controls regarding monitoring access to the WebTA application, including a process to review, approve, and recertify USSS personnel with certain access roles within the application, were not properly designed and implemented and documentation was not maintained supporting user access roles.

Recommendations

We recommend that the USSS 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 USSS' financial management systems and associated IT security program (in accordance with USSS and DHS requirements, as applicable):

Access Controls

- Update the USSS WebTA manual to include formal policy and access documentation that will cover WebTA role request, approval, and monitoring.

OBSERVATIONS RELATED TO NON-TECHNICAL INFORMATION SECURITY

To complement our IT controls test work during the FY 2015 audit, we performed additional non-technical information security procedures at USSS. These procedures included after-hours physical security walkthroughs to identify instances where USSS 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 2015 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.

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 USSS 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 USSS 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 USSS, DHS OIG, and DHS OCIO.

During after-hours physical security walkthroughs performed at USSS, we inspected a total of 42 workspaces. Of those, 22 were observed to have material – including, but not limited to, system passwords, information marked “FOUO”, documents containing sensitive PII, and government-issued laptops or storage media – left unattended and unsecured after business hours in violation of DHS policy.

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

Department of Homeland Security
Information Technology Management Letter
U.S. Secret Service
September 30, 2015

Appendix A

Description of Key USSS Financial Systems and IT Infrastructure within the Scope of the FY 2015 DHS Financial Statement Audit

Department of Homeland Security
Information Technology Management Letter
U.S. Secret Service
September 30, 2015

Below is a description of the significant USSS financial management systems and supporting IT infrastructure included in the scope of the FY 2015 DHS financial statement audit.

Web Time and Attendance (WebTA)

WebTA is a commercial off-the-shelf (COTS) web-based major application hosted by the United States Department of Agriculture (USDA) National Finance Center (NFC) and developed, operated, and maintained by the NFC IT Services Division and NFC Risk Management Staff. DHS components utilize NFC and WebTA to process front-end input and certification of time and attendance entries by the DHS user community to facilitate payroll processing.

Department of Homeland Security
Information Technology Management Letter
U.S. Secret Service
September 30, 2015

Appendix B

FY 2015 IT Notices of Findings and Recommendations at USSS

Department of Homeland Security
Information Technology Management Letter
U.S. Secret Service
September 30, 2015

| FY 2015 NFR # | NFR Title | FISCAM Control Area | New Issue | Repeat Issue |
|----------------------|---|----------------------------|------------------|---------------------|
| USSS-IT-15-01 | Security Awareness Issues Identified during After-Hours Physical Security Testing at USSS | Security Management | | X |
| USSS-IT-15-02 | WebTA Account Management Policies and Procedures | Access Controls | 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

U.S. Secret Service

Director
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