OFFICE OF INSPECTOR GENERAL

Information Technology Management Letter for the United States Secret Service Component of the FY 2016 Department of Homeland Security Financial Statement Audit

Homeland Security

June 15, 2017
OIG-17-72

DHS OIG HIGHLIGHTS

Information Technology Management Letter for the United States Secret Service Component of the FY 2016 Department of Homeland Security Financial Statement Audit

June 15, 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 USSS, in coordination with the DHS Chief Information Officer and Acting 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

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 (GITC) and business process application controls at the United States Secret Service (USSS). KPMG continued to identify GITC deficiencies at USSS related to access controls, segregation of duties, and configuration management.

The deficiencies collectively limited USSS' 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 identified in the FY 2016 DHS Agency Financial Report.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

June 15, 2017

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 2016 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 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,
U.S. Department of Homeland Security, and
Chief Information Officer and Chief Financial Officer,
U.S. Secret Service,
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 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.

We also noted certain internal control deficiencies at USSS 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 USSS, we noted certain matters in the general IT control areas of access controls, segregation of duties, 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 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 systems and IT infrastructure within the scope of the Fiscal Year (FY) 2016 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, 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 USSS 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 USSS' 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
U.S. Secret Service
September 30, 2016

TABLE OF CONTENTS

APPENDICES

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 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

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 five FISCAM categories was 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 that depend on the completeness, accuracy, and integrity of information provided by the entity in support of our financial audit procedures. Consequently, FY 2016 GITC procedures evaluated at USSS 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 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.

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 2016 DHS *Security Testing Authorization Letter* (STAL) signed by KPMG LLP, 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 2016 DHS financial statement audit.

SUMMARY OF FINDINGS

During our FY 2016 assessment of GITCs and IT application controls, we continued to identify GITC deficiencies at USSS related to access controls, segregation of duties, and configuration management. In many cases, new control deficiencies reflected weaknesses over new systems and controls in scope for FY 2016.

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 their confidentiality, integrity, and availability. In addition, certain of these deficiencies at USSS 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 14 IT Notices of Findings and Recommendations (NFR) issued during our FY 2016 testing at USSS, two were repeat findings, either wholly or in part from the prior year, and 12 were new findings. The 14 IT NFRs issued represent deficiencies and observations related to four 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 USSS policies, financial system controls lacked proper documentation, were not fully designed and implemented, were inadequately detailed, and were inconsistently implemented. The most significant weaknesses from a financial statement audit perspective continued to include unauthorized or inadequately monitored access to, and activity within, system components for key USSS financial applications.

Although the recommendations made by us should be considered by USSS, it is ultimately the 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 2016 DHS consolidated financial statements, we identified the following GITC deficiencies at USSS:

Access Controls

- Controls related to the account management process were not designed and implemented or operating effectively. Deficiencies included not maintaining account management documentation for initial account creation; a supervisor unaware of a role assigned to a user; and inadequate account management documentation including procedures for creating accounts for all user roles within the system.

- Account management procedures were not documented for privileged users of the application and the database.

- Strong password requirements were not consistently enforced in compliance with DHS policies on passwords for databases supporting financial applications, as well as for the initial application account password synchronizing the user account to the network account.

- Controls related to audit logs were not operating effectively, including operating system logs not being reviewed on a consistent basis, and both operating system and database logs not being reviewed by individuals separate from the system administrator group.

- Controls related to recertification of user accounts on the application, database, and operating system were not designed or operating effectively. Deficiencies included not documenting the process for user recertification, not performing full recertification of all users, and not maintaining documentation supporting user recertification.

- Application users were not timely removed upon their separation from USSS, and a complete and accurate listing of separated contractors could not be provided.

Configuration Management

- Certain configuration-related deficiencies identified on servers, workstations, and system software were not remediated timely and tracked appropriately for remediation within management's Plan of Action and Milestones (POA&M).

Segregation of Duties

- An overall weakness regarding segregation of duties had been identified by management.

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

- Develop and follow a standard operating procedure for provisioning accounts, and document all user roles and the required approval for those roles.
- Update account management procedures to address application privileged users and database privileged users.
- Review and update password requirements to be in compliance with DHS policy.
- Update policies and procedures around audit logging to include segregations of duties for review, and review and update the audit log management tool configuration.
- Define, create/update, and implement procedural documentation around recertification of user accounts.
- Review and revise the policy and procedures for out-processing separated employees and contractors.

Configuration Management

- Implement an automated patching solution and updated USSS policy to address vulnerability management and remediation.

Segregation of Duties

- Update application and database account management processes and associated segregation of duties definitions, as well as system administrator processes.

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 USSS. These procedures included after-hours physical security walkthroughs and social engineering 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 2016 *Security Testing Authorization Letter* (STAL) signed by DHS OIG management, KPMG management, and DHS management.

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 USSS personnel were willing to divulge network or system passwords that, if exploited, could compromise sensitive USSS information.

To conduct this testing, we made phone calls from various USSS locations at various times throughout the audit. Posing as USSS technical support personnel, we attempted to solicit access credentials from USSS users. Attempts to log into USSS 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 USSS, we attempted to call a total of 33 employees and contractors and reached 11. Of those 11 individuals with whom we spoke, two individuals divulged passwords in violation of DHS policy.

The selection of attempted or connected calls was not statistically derived, and, therefore, the results described here should not be used to extrapolate to USSS 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 (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 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 USSS, DHS OIG, and DHS OCIO.

During after-hours physical security walkthroughs performed at USSS, we inspected a total of 55 workspaces. Of those, 19 were observed to have material – including, but not limited to, unsecured laptops and external media, system passwords and access credentials, 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, and, therefore, the results described here should not be used to extrapolate to USSS as a whole.

Appendix A

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

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

Travel Manager, Oracle Financials, Compusearch/PRISM, and Sunflower (TOPS)

TOPS is an enterprise financial management system that supports acquisition, accounting, travel, and property management functions. TOPS is a single, comprehensive, integrated financial management system that all of USSS, including field offices, uses.

Oracle databases and Microsoft Windows, Solaris, and Red Hat Linux-based servers support TOPS, and it is located in Washington, DC.

Web Time and Attendance (WebTA)

WebTA is a commercial off-the-shelf web-based major application that the United States Department of Agriculture's National Finance Center (NFC) hosts. The NFC's IT Services Division and NFC Risk Management Staff developed, operate, and maintain it. USSS uses WebTA to process front-end input and certification of time and attendance entries by the USSS user community to facilitate payroll processing.

Appendix B

FY 2016 IT Notices of Findings and Recommendations at USSS

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
USSS-IT-16-01	Security Awareness Issues Identified During After-Hours Physical Security Testing at USSS Headquarters	Security Management		X
USSS-IT-16-02	Ineffective Profile Settings and Controls for TOPS Database Security	Access Controls	X	
USSS-IT-16-03	Ineffective Controls Over TOPS Database and Operating System Security Audit Log Review	Access Controls	X	
USSS-IT-16-04	Ineffective Design Over TOPS Operating System Administrator Account Recertification	Access Controls	X	
USSS-IT-16-05	Inadequate Documentation for TOPS Application and Database Privileged User Account Management	Access Controls	X	
USSS-IT-16-06	Inadequate Controls over USSS' Instance of Web Time and Attendance (WebTA)	Access Controls		X
USSS-IT-16-07	Weakness in TOPS Segregation of Duties	Segregation of Duties	X	
USSS-IT-16-08	Security Awareness Issues Identified during Social Engineering Testing at USSS	Security Management	X	
USSS-IT-16-09	Weakness in TOPS Application Authentication	Access Controls	X	
USSS-IT-16-10	Ineffective Design Over TOPS Database Administrator Account Recertification	Access Controls	X	
USSS-IT-16-11	Inadequate Documentation for TOPS Operating System Privileged User Account Management	Access Controls	X	
USSS-IT-16-12	Inadequate Design Over TOPS Application User Account Recertification	Access Controls	X	

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
USSS-IT-16-13	Ineffective Controls Over Timely Removal of Accounts for Terminated Individuals within TOPS	Access Controls	X	
USSS-IT-16-14	Security Management and Configuration Management Controls – Vulnerability Assessment	Configuration Management	X	

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

Acting Chief Financial Officer
Chief Information Officer
Audit Liaison

United States 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