OFFICE OF INSPECTOR GENERAL

Information Technology Management Letter for the National Protection and Programs Directorate of the FY 2016 Department of Homeland Security Financial Statement Audit

Homeland Security

June 22, 2017
OIG-17-78

DHS OIG HIGHLIGHTS

Information Technology Management Letter for the National Protection and Programs Directorate Component of the FY 2016 Department of Homeland Security Financial Statement Audit

June 22, 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 NPPD, 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 National Protection and Programs Directorate (NPPD). KPMG continued to identify GITC deficiencies at NPPD related to access controls and configuration management.

The deficiencies collectively limited NPPD'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 22, 2017

MEMORANDUM FOR: Scott Libby
Acting Chief Information Officer
National Protection and Programs Directorate

David Hill
Acting Director Budget and Financial Administration
National Protection and Programs Directorate

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

SUBJECT: *Information Technology Management Letter for the National Protection and Programs Directorate 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 National Protection and Programs Directorate 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,
National Protection and Programs Directorate,
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 National Protection and Programs Directorate (NPPD), 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 NPPD 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 NPPD, we noted certain matters 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*.*

We have provided a description of key NPPD 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 NPPD 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 NPPD, including certain deficiencies in internal control that we consider to be significant deficiencies and 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 DHS Office of Inspector General (OIG) and the NPPD 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 NPPD'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
National Protection and Programs Directorate
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 National Protection and Programs Directorate (NPPD), a component of DHS, to assist in planning and performing our audit engagement.

Scope and Approach

<u>General Information Technology Controls</u>

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 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 NPPD 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.

Financial System Functionality

In recent years, we have noted that limitations in NPPD's 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. NPPD's financial system is hosted by its service provider, U.S. Immigration and Customs Enforcement (ICE). Therefore, in FY 2016, we continued to evaluate and consider the impact of financial system functionality on internal control over financial reporting.

Appendix A provides a description of the key NPPD 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 identified GITC deficiencies at NPPD related to access controls and configuration management. NPPD's main financial application is owned and operated ICE. As a service provider, ICE provides support to NPPD. The GITC deficiencies we identified at ICE could potentially impact NPPD's financial data, and as such, we issued a finding to NPPD.

The conditions supporting our findings collectively limited NPPD's ability to ensure that critical financial and operational data were maintained in such a manner to ensure their confidentiality, integrity, and availability. In addition, certain of these deficiencies at NPPD 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 five IT Notices of Findings and Recommendations (NFR) issued during our FY 2016 testing at NPPD, one was a repeat finding, either wholly or in part from the prior year, and four were new findings. The five IT NFRs issued represent deficiencies and observations related to two 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 NPPD 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 included the lack of account management policies.

During our IT audit procedures, we also evaluated and considered the impact of financial system functionality on financial reporting. In recent years, we have noted that limitations in NPPD's financial systems' functionality may be inhibiting NPPD's ability to implement and maintain effective internal control and effectively and efficiently process and report financial data. The key financial system has not been substantially updated since being inherited from legacy agencies several years ago. Key NPPD financial systems were not compliant with Federal financial management system requirements as defined by the *Federal Financial Management Improvement Act of 1996* (FFMIA) and Office of Management and Budget Circular Number A-123 Appendix D, *Compliance with FFMIA*.

Although the recommendations made by us should be considered by NPPD, it is ultimately the responsibility of NPPD 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 NPPD:

Access Controls

- A complete and accurate listing of contractors separated during the fiscal year could not be produced.
- Account management policies did not exist or were lacking sufficient detail in areas such as segregation of duties, recertification, elevated privileges, and disabling accounts upon user separation.
- Supporting account access authorization documentation was not provided or was not properly documented.

Access Controls and Configuration Management

- Deficiencies existed regarding non-compliance with DHS policy for database password configurations, non-compliance with delegation of authority requirements, a lack of account management policies and procedures for privileged user access to operating systems and databases, an inadequate privileged user semi-annual recertification process, insufficient audit log controls for the operating system, incomplete documentation for configuration management controls, and weaknesses in vulnerability scanning activities.

Recommendations

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

Access Controls

- Formalize procedures for monitoring contractor onboarding and off boarding.
- Update and formalize account management process documentation and confirm that access forms exist for the application.
- Review user accounts bi-weekly.

Access Controls and Configuration Management

- Work with ICE Chief Information Officer (CIO) and Chief Financial Officer (CFO) to monitor remediation of the GITC deficiencies and request regular reporting from ICE.
- Implement complementary user entity controls.

Appendix A

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

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

Federal Financial Management System (FFMS)

FFMS is a mainframe-based major application and the official accounting system of record for NPPD. It is used to create and maintain a record of each allocation, commitment, obligation, travel advance, and accounts receivable. The system supports all internal and external financial reporting requirements.

On behalf of NPPD, ICE OCIO hosts and supports the various instances of FFMS that NPPD uses exclusively for the NPPD user community and, on a limited basis, for the ICE OCIO and finance center personnel providing support services for NPPD.

The application is hosted at Datacenter 2 in Clarksville, VA, and the IBM z/OS mainframe and Oracle databases support it.

Federal Protective Service Data System (FPSDS)

FPSDS is used to generate monthly security guard bills for other Federal agencies that use NPPD services.

The application is hosted at Datacenter 2 in Clarksville, VA, and an SQL Server database and Windows servers support it.

Web Time and Attendance (WebTA)

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

EmpowHR

EmpowHR is a COTS web-based major application that USDA NFC hosts. The NFC IT Services Division and NFC Risk Management Staff developed, operate, and maintain it. NPPD uses NFC and EmpowHR to initiate, authorize, and send personnel data to NFC for processing.

Appendix B

FY 2016 IT Notices of Findings and Recommendations at NPPD

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
NPPD-IT-16-01	Weakness with WebTA Account Management Controls	Access Controls	X	
NPPD-IT-16-02	Federal Protective Service Data System (FPSDS) Account Management Weakness	Access Controls	X	
NPPD-IT-16-03	Inability to Generate a Complete and Accurate Listing of Separated Contractors	Access Controls		X
NPPD-IT-16-04	Weakness with EmpowHR Account Management Controls	Access Controls	X	
NPPD-IT-16-05	Federal Financial Management System Deficiencies at ICE that Impact NPPD Operations	Access Controls and 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

National Protection and Programs Directorate

Senior Official Performing the Duties of the Under Secretary
Acting Director Budget & Financial Administration
Acting 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