

**Information Technology  
Management Letter for the  
National Protection and  
Programs Directorate  
Component of the FY 2015  
Department of Homeland  
Security Financial Statement  
Audit**





# DHS OIG HIGHLIGHTS

## *Information Technology Management Letter for the National Protection and Programs Directorate Component of the FY 2015 Department of Homeland Security Financial Statement Audit*

---

**May 10, 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 NPPD, 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 for the year ended September 30, 2015. KPMG, LLP evaluated selected general IT controls and business process application controls at the National Protection and Programs Directorate (NPPD). KPMG, LLP identified a general IT control deficiency at NPPD related to access controls.

The conditions supporting our finding collectively limited NPPD's 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

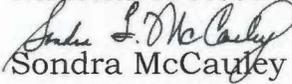
Department of Homeland Security

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

May 10, 2016

MEMORANDUM FOR: David Epperson  
Chief Information Officer  
National Protection and Programs Directorate

David Hill  
Chief Financial Officer  
National Protection and Programs Directorate

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

SUBJECT: *Information Technology Management Letter for the  
National Protection and Programs Directorate  
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 National Protection and Programs Directorate 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,  
National Protection and Programs Directorate,  
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 National Protection and Programs Directorate (NPPD), a component of DHS, which 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 NPPD, we noted certain internal control deficiencies in the general information technology (IT) control areas of access controls. These matters are described in the *Finding and Recommendation* section of this letter.

We have provided a description of key NPPD financial systems and IT infrastructure within the scope of the FY 2015 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 Office of Inspector General and the NPPD 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 NPPD's 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*  
*National Protection and Programs Directorate*  
September 30, 2015

---

**TABLE OF CONTENTS**

	<b>Page</b>
Objective, Scope, and Approach	2
Summary of Finding	4
Finding and Recommendation	5
Finding	5
Recommendation	5

**APPENDICES**

<b>Appendix</b>	<b>Subject</b>	<b>Page</b>
<b>A</b>	Description of Key NPPD Financial System and IT Infrastructure within the Scope of the FY 2015 DHS Financial Statement Audit	6
<b>B</b>	FY 2015 IT Notice of Finding and Recommendation at NPPD	8

## **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 National Protection and Programs Directorate (NPPD), a component of DHS, to assist in planning and performing our audit engagement.

### **Scope and Approach**

#### General Information Technology 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 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

Department of Homeland Security  
*Information Technology Management Letter*  
*National Protection and Programs Directorate*  
September 30, 2015

---

information provided by the entity in support of our financial audit procedures. Consequently, FY 2015 GITC procedures at NPPD 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 IT application controls (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 business process application controls 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.

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 2015, we continued to evaluate and consider the impact of financial system functionality on internal control over financial reporting.

Department of Homeland Security  
*Information Technology Management Letter*  
*National Protection and Programs Directorate*  
September 30, 2015

---

**SUMMARY OF FINDING**

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

The conditions supporting our finding collectively limited NPPD's ability to ensure that critical financial and operational data were maintained in such a manner as to ensure confidentiality, integrity, and availability. The one IT NFR issued represents deficiencies and observations related to one of the five FISCAM GITC categories.

The finding resulted from the lack of fully designed and implemented 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 NPPD policies and procedures, as applicable.

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

## **FINDING AND RECOMMENDATION**

### **Finding**

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

#### *Access Controls*

- A complete and accurate listing of contractors separated during the fiscal year cannot be produced.

### **Recommendation**

We recommend that the NPPD Security Office in coordination with the DHS Chief Security Office, make the following improvement to NPPD's financial management systems and associated IT security program (in accordance with NPPD and DHS requirements, as applicable):

#### *Access Controls*

- Develop an effective process to track active and separated contractors and also active and separated employees.

Department of Homeland Security  
*Information Technology Management Letter*  
*National Protection and Programs Directorate*  
September 30, 2015

---

## **Appendix A**

### **Description of Key NPPD Financial System and IT Infrastructure within the Scope of the FY 2015 DHS Financial Statement Audit**

Department of Homeland Security  
*Information Technology Management Letter*  
*National Protection and Programs Directorate*  
September 30, 2015

---

Below is a description of the NPPD's significant financial management system and supporting IT infrastructure included in the scope of the FY 2015 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.

The various instances of FFMS that NPPD uses are hosted and supported by the ICE Office of the Chief Information Officer (OCIO) on behalf of NPPD, exclusively for internal use by the NPPD user community and, on a limited basis, ICE OCIO and finance center personnel performing support services for NPPD.

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

Department of Homeland Security  
*Information Technology Management Letter*  
*National Protection and Programs Directorate*  
September 30, 2015

---

## **Appendix B**

### **FY 2015 IT Notice of Finding and Recommendation at NPPD**

Department of Homeland Security  
*Information Technology Management Letter*  
*National Protection and Programs Directorate*  
September 30, 2015

---

<b>FY 2015 NFR #</b>	<b>NFR Title</b>	<b>FISCAM Control Area</b>	<b>New Issue</b>	<b>Repeat Issue</b>
NPPD-IT-15-01	Inability to Generate a Complete and Accurate Listing of Separated Contractors	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

**National Protection and Program Directorate**

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](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