OFFICE OF INSPECTOR GENERAL

Information Technology Management Letter for the Federal Law Enforcement Training Center Component of the FY 2014 Department of Homeland Security Financial Statement Audit

Homeland Security

April 23, 2015

OIG-15-79

HIGHLIGHTS

Information Technology Management Letter for the Federal Law Enforcement Training Center Component of the FY 2014 Department of Homeland Security Financial Statement Audit

April 23, 2015

Why We Did This

Each year, our independent auditors identify component-level information technology control deficiencies as part of the DHS consolidated financial statement audit. This letter provides details not included in the FY 2014 DHS Agency Financial Report.

What We Recommend

We recommend that FLETC, in coordination with the DHS Chief Information Officer and the Chief Financial Officer, make improvements to the financial management systems and associated information technology security program at FLETC, as well as DHS components it supports.

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, 2014. KPMG LLP evaluated selected general information technology controls and business process application controls at the Federal Law Enforcement Training Center (FLETC), the Office of Intelligence & Analysis (I&A), and the Office of Operations Coordination and Planning (OPS). FLETC provides financial system hosting and support to I&A and OPS. KPMG LLP determined that FLETC, I&A, and OPS had made improvements in designing and consistently implementing controls related to reviewing audit logs and enforcing account security requirements.

However, KPMG LLP continued to identify general information technology control deficiencies related to logical access to core financial systems at FLETC, I&A, and OPS. Such control deficiencies limited the ability to ensure the confidentiality, integrity, and availability of critical financial and operational data.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC

April 23, 2015

TO: Sandy Peavy
Chief Information Officer
Federal Law Enforcement Training Center

Donald R. Lewis
Chief Financial Officer
Federal Law Enforcement Training Center

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

SUBJECT: *Information Technology Management Letter for the Federal Law Enforcement Training Center Component of the FY 2014 Department of Homeland Security Financial Statement Audit*

Attached for your information is our final report, *Information Technology Management Letter for the Federal Law Enforcement Training Center Component of the FY 2014 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 2014 Financial Statements and Internal Control over Financial Reporting*, dated November 14, 2014, which was included in the FY 2014 DHS Agency Financial Report.

The independent public accounting firm KPMG LLP conducted the audit of DHS' FY 2014 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 Division, at (202) 254-5451.

Attachment

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

December 19, 2014

Office of Inspector General,
U.S. Department of Homeland Security, and
Chief Information Officer and Chief Financial Officer,
Federal Law Enforcement Training Center
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, 2014 (hereinafter, referred to as the "fiscal year (FY) 2014 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. 14-02, *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 Federal Law Enforcement Training Center (FLETC), a component of DHS, as well as the Office of Intelligence & Analysis (I&A) and the Office of Operations Coordination and Planning (OPS), components of DHS that receive financial system hosting and support from FLETC, 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 FLETC, as well as at I&A and OPS, we noted certain internal control deficiencies in the general IT control area of access controls. These matters are described in the *Findings and Recommendations* section of this letter.

We have provided a description of key FLETC, I&A, and OPS financial systems and IT infrastructure within the scope of the FY 2014 DHS financial statement audit in Appendix A, and a listing of each FLETC, I&A, and OPS 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 FLETC, I&A, and OPS, 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 FLETC Chief Financial Officer.

Our audit procedures are designed primarily to enable us to form opinions on the FY 2014 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 the FLETC, I&A, and OPS organizations 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
Federal Law Enforcement Training Centers
September 30, 2014

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE, AND APPROACH

Objective

We have audited the consolidated financial statements of the U.S. Department of Homeland Security (DHS or Department) for the year ended September 30, 2014 (hereinafter, referred to as the "fiscal year (FY) 2014 DHS consolidated financial statements"). In connection with our audit of the FY 2014 DHS consolidated financial statements, we performed an evaluation of selected general information technology (IT) controls (GITCs) and business process application controls (BPACs) at the Federal Law Enforcement Training Centers (FLETC), the Office of Intelligence & Analysis (I&A), and the Office of Operations Coordination and Planning (OPS), components 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 of 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 to 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 which depend on the completeness, accuracy, and integrity of information provided by the entity in support of our financial audit procedures. Consequently, FY 2014 GITC procedures at FLETC, I&A, and OPS 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 which 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 relate 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 FLETC, I&A, and OPS financial systems' functionality may be inhibiting the agencies' ability to implement and maintain internal controls, including effective GITCs and BPACs supporting financial data processing and reporting. Many key financial and feeder systems have not been substantially updated since being inherited from legacy agencies several years ago. Therefore, in FY 2014, 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 FLETC, I&A, and OPS financial systems and IT infrastructure within the scope of the FY 2014 DHS financial statement audit.

SUMMARY OF FINDINGS

During FY 2014, we noted that FLETC took corrective action to address certain prior year IT control deficiencies. For example, FLETC made improvements over designing and consistently implementing controls related to the review of audit logs and the enforcement of account security requirements. However, we continued to identify GITC deficiencies related to access controls for FLETC's, I&A's, and OPS' core financial systems.

The conditions supporting our findings collectively limited FLETC's, I&A's, and OPS' ability to ensure that critical financial and operational data were maintained in such a manner as to ensure confidentiality, integrity, and availability. Of the three IT Notices of Findings and Recommendations (NFRs) issued during our FY 2014 testing at FLETC, I&A, and OPS, all were repeat findings, either partially or in whole from the prior year.

The majority of the findings resulted from the lack of properly documented, fully designed , 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 FLETC, I&A, and OPS policies and procedures, as applicable. The most significant weaknesses from a financial statement audit perspective continued to include inadequately monitored access to system components for the key FLETC, I&A, and OPS financial applications.

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 FLETC, I&A, and OPS financial systems functionality may be inhibiting FLETC's and I&A/OPS' ability to implement and maintain effective internal control and to effectively and efficiently process and report financial data. Many key financial and feeder systems have not been substantially updated since being inherited from legacy agencies several years ago.

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

FINDINGS AND RECOMMENDATIONS

Findings

During our audit of the FY 2014 DHS consolidated financial statements, we identified the following GITC deficiencies at FLETC, I&A, and OPS:

Access Controls

- FLETC, I&A, and OPS management did not maintain listings of separated contractors to support proper monitoring controls over contractor access to the respective financial application environments.

- Documentation supporting account management activities, including revocation of access for separating individuals on I&A and OPS financial applications, was not consistently maintained in accordance with established procedures requiring such documentation at the time that access changes are processed.

Recommendations

We recommend that the FLETC 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 FLETC, I&A, and OPS financial management systems and associated IT security program (in accordance with FLETC and DHS requirements, as applicable):

Access Controls

- Implement monitoring controls over the account management process specific to FLETC, I&A, and OPS contractors, including periodic notification of separated or transferred contractors and periodic revalidation of authorized contract personnel, to ensure that access to financial applications remains current and commensurate with job responsibilities.

- Implement or enhance existing technical and monitoring controls over processes related to personnel separation to ensure that system owners are notified and revoke access to affected accounts timely.

Appendix A

Description of Key FLETC, I&A, and OPS Financial Systems and IT Infrastructure within the Scope of the FY 2014 DHS Financial Statement Audit

Below is a description of the significant FLETC, I&A, and OPS financial management system and supporting IT infrastructure included in the scope of the FY 2014 DHS financial statement audit.

Financial Accounting and Budgeting System (FABS)

FABS is a web-based, major application and the official accounting system of record for FLETC, I&A, and OPS. An instance of this commercial off-the-shelf financial processing system, known as Momentum, is used to input requisitions, approve receipt of property, and manage property asset records and financial records for contracts, payments, payroll, and budgetary transactions. It contains interfaces with external service providers, including the United States Department of Agriculture's National Finance Center and the General Services Administration's Concur Government Edition electronic travel system.

FLETC provides financial management services to I&A and OPS through a separately-hosted instance of the FABS environment (under the terms established through a Memorandum of Understanding between the two components), which was developed to mirror the FLETC FABS environment.

FABS is hosted and supported by the FLETC IT Infrastructure Branch and the FLETC OCFO Finance Division (on behalf of I&A and OPS, under the terms established in a Memorandum of Understanding between the two components) exclusively for internal use by the FLETC, I&A, and OPS user communities.

Appendix B

FY 2014 IT Notices of Findings and Recommendations at FLETC, I&A, and OPS

FY 2014 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FLETC-IT-14-01	FLETC Contractor Separation Listing	Access Controls		X
IAOPS-IT-14-01	Contractor Separation Listing	Access Controls		X
IAOPS-IT-14-02	Separation Process	Access Controls		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

Federal Law Enforcement Training Center

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