Department of Homeland Security

Office of Inspector General

Information Technology Management Letter for the FLETC Component of the FY 2013 Department of Homeland Security Financial Statement Audit

OIG-14-84

April 2014

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

April 29, 2014

MEMORANDUM FOR: Sandy Peavy
Chief Information Officer
Federal Law Enforcement Training Center

Donald R. Lewis
Assistant Director
Federal Law Enforcement Training Center

FROM: Richard Harsche
Acting Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the Federal Law Enforcement Training Center Component of the FY 2013 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 2013 Department of Homeland Security Financial Statement Audit.* This report contains comments and recommendations related to information technology internal control deficiencies that were not required to be reported in the Independent Auditors' Report.

We contracted with the independent public accounting firm KPMG LLP (KPMG) to conduct the audit of Department of Homeland Security fiscal year (FY) 2013 consolidated financial statements. The contract required that KPMG perform its audit according to generally accepted government auditing standards and guidance from the Office of Management and Budget and the Government Accountability Office. KPMG is responsible for the attached management letter dated March 11, 2014, and the conclusion expressed in it.

Please call me with any questions, or your staff may contact Sharon Huiswoud, Director, Information Systems Audit Division, at (202) 254-5451.

Attachment

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

March 11, 2014

Office of Inspector General,
U.S. Department of Homeland Security, and
Chief Information Officer and Chief Financial Officer,
U.S. Department of Homeland Security Federal Law Enforcement Training Center

Ladies and Gentlemen:

We have audited the financial statements of the U.S. Department of Homeland Security (DHS or Department) for the year ended September 30, 2013 (referred to herein as the "fiscal year (FY) 2013 financial statements"), and have issued our report thereon dated December 11, 2013. In planning and performing our audit of the financial statements of DHS, in accordance with auditing standards generally accepted in the United States of America and *Government Auditing Standards*, 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 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.

In accordance with *Government Auditing Standards*, our *Independent Auditors' Report*, dated December 11, 2013, included internal control deficiencies identified during our audit that, in aggregate, represented a material weakness in information technology (IT) controls and financial system functionality at the DHS Department-wide level. This letter represents the separate limited distribution report mentioned in that report, of matters related to the Federal Law Enforcement Training Center (FLETC) and the Offices of Intelligence & Analysis and Operations Coordination and Planning (I&A/OPS).

During our audit we noted certain matters involving internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management and communicated through Notices of Findings and Recommendations (NFRs), are intended to improve internal control or result in other operating efficiencies and are summarized as described below.

With respect to FLETC's and I&A/OPS' financial systems' IT controls, we noted certain matters in the areas of access controls, segregation of duties, and IT application controls. These matters are described in the *General IT Control Findings and Recommendations* and *IT Application Controls* sections of this letter.

The Table of Contents identifies each section of the letter. We have provided a description of key FLETC and I&A/OPS financial systems and IT infrastructure within the scope of the FY 2013 DHS financial statement audit in Appendix A, and a listing of each IT NFR 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, 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 DHS Chief Financial Officer.

Our audit procedures are designed primarily to enable us to form an opinion on the 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
Federal Law Enforcement Training Center
September 30, 2013

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE, AND APPROACH

Objective

We have audited the financial statements of the U.S. Department of Homeland Security (DHS or Department) for the fiscal year that ended on September 30, 2013 (referred to herein as the "fiscal year (FY) 2013 financial statements"). In connection with our audit of the FY 2013 financial statements, we performed an evaluation of selected general information technology (IT) controls (GITCs) and IT application controls at the Federal Law Enforcement Training Center (FLETC) and the Offices of Intelligence & Analysis and Operations Coordination and Planning (I&A/OPS) to assist in planning and performing our audit engagement.

Scope

The scope of our GITC and IT application control test work is described in Appendix A, which provides a description of the key FLETC and I&A/OPS financial systems and IT infrastructure within the scope of the FLETC component of the FY 2013 DHS consolidated financial statement audit.

Approach

General Information Technology Controls

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

- *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.

- *Access Control* – Controls that limit or detect access to computer resources (data, programs, equipment, and facilities) and protect against unauthorized modification, loss, and disclosure.

- *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.

    - We performed technical information security testing for key FLETC network and system devices. The technical security testing was performed from within select DHS facilities and focused on

production devices that directly support DHS' and FLETC's financial processing and key general support systems.

- *Segregation of Duties* – Controls that constitute policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations.

- *Contingency Planning* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

IT Application Controls

We performed testing over selected key IT application controls 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 application controls as the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, or payroll.

SUMMARY OF FINDINGS

During FY 2012, FLETC took corrective action to address certain prior year IT control deficiencies. For example, FLETC made improvements over strengthening controls around segregation of duties and configuration management. However, during FY 2013, we continued to identify GITC deficiencies that could potentially impact FLETC's and I&A/OPS' financial data related to controls over access control, segregation of duties, and IT application controls for the FLETC and I&A/OPS core financial and feeder systems and associated General Support System environments.

Collectively, the IT control deficiencies limited FLETC's and I&A/OPS' ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these deficiencies negatively impacted the internal controls over FLETC's and I&A/OPS' financial reporting and its operations.

Of the eleven IT Notices of Findings and Recommendations (NFRs) issued during our FY 2013 testing, one was a repeat finding from the prior year, and ten were new findings. The eleven IT NFRs issued represent deficiencies in two of the five FISCAM GITC categories as well as in the area of IT application controls.

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 DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program,* requirements and National Institute of Standards and Technology guidance. Specifically, the findings stem from:

1. Inadequately designed and ineffective access control policies and procedures relating to the management of logical access to financial applications, databases, and support systems;
2. Insufficient logging of system events and monitoring of audit logs; and
3. Improper configuration of application controls to prevent recording of improper expenses.

These deficiencies may increase the risk that the confidentiality, integrity, and availability of system controls and FLETC's and I&A/OPS' financial data could be exploited, thereby compromising the integrity of FLETC and I&A/OPS financial data used by management and reported in FLETC's, I&A/OPS', and DHS' financial statements.

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

GENERAL IT CONTROL FINDINGS AND RECOMMENDATIONS

Findings

During our audit of the FY 2013 DHS financial statements, we identified the following FLETC and I&A/OPS GITC deficiencies.

Access Controls

- Audit logs for the FLETC and I&A/OPS Momentum applications were not consistently or timely reviewed by management in accordance with DHS and FLETC policy.
- DHS requirements for password complexity were not fully implemented for accounts on the Glynco Administrative Network (GAN).
- FLETC and IA&OPS management did not maintain listings of separated contractors to support proper monitoring controls around contractor access to the respective Momentum environments.
- Account management activities on the FLETC and I&A/OPS Momentum environments, including implementation of account inactivity controls, authorization of profile changes, deactivation of accounts, and management of generic accounts, were not consistently or timely implemented or documented in accordance with FLETC policy.

Segregation of Duties

- FLETC personnel were granted access to the I&A/OPS Momentum application environment and supporting system infrastructure, including highly-privileged administrative and access, that was inconsistent with the segregation of duties principles defined by DHS policy.

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's and I&A/OPS' financial management systems and associated IT security program.

Access Controls

- Implement monitoring controls over the audit log review process to ensure that all required auditable events are being reviewed by management on a periodic basis, are documented, and audit log review evidence is maintained in accordance with DHS and FLETC requirements.
- Implement technical controls to ensure that passwords for GAN accounts are configured in accordance with DHS requirements.

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

- Implement technical controls to enforce DHS and FLETC requirements related to implementation of account inactivity controls, and implement monitoring controls to review and ensure continued compliance with account inactivity requirements.

- Implement monitoring controls over the account management process to ensure that granting, modification and revocation of access to the FLETC and I&A/OPS Momentum environments, including generic accounts, are authorized, documented, and performed timely and in accordance with DHS and FLETC requirements.

Segregation of Duties

- Implement additional monitoring controls over I&A/OPS Momentum access, in particular for highly-privileged and administrative access, to ensure that segregation of duties principles are enforced in accordance with DHS and FLETC policy.

IT APPLICATION CONTROLS

During the FLETC and I&A/OPS component of the FY 2013 DHS financial statement audit, we identified the following IT application control and financial system functionality deficiency:

Finding

- The I&A/OPS instance of the Momentum application lacked controls to prevent or detect the processing of multiple payment vouchers referencing the same invoice, which could result in the recording of improper expenses in the general ledger.

Recommendation

- While we noted that FLETC management corrected the deficiency described above, we recommend that the FLETC OCFO and OCIO, in coordination with the DHS OCFO and the DHS OCIO, continue to implement appropriate monitoring controls to ensure that required system configurations, including the invoice control tolerance settings, are properly implemented to ensure the continued effectiveness of preventative or detective controls related to key financial line items and assertions material to the DHS consolidated financial statements.

Appendix A

Description of Key FLETC and I&A/OPS Financial Systems and IT Infrastructure within the Scope of the FY 2013 DHS Financial Statement Audit

Below is a description of significant FLETC and I&A/OPS financial management systems and supporting IT infrastructure included in the scope of the FLETC and I&A/OPS component of the DHS FY 2013 financial statement audit.

Financial Accounting and Budgeting System (FABS)

The FLETC FABS application (also referred to as Momentum) is an all-in-one financial processing system. It functions as the computerized accounting and budgeting system for FLETC. FLETC provides financial management services to I&A/OPS through a separately hosted Momentum environment, which was developed to mirror the FLETC Momentum environment. The FABS system exists to provide all of the financial and budgeting transactions in which FLETC is involved. FABS system users are from all FLETC sites that input requisitions and managers that approve receipt of property and manage the property asset records and financial records for contracts, payments, payroll, and budgetary transactions. Hosted on a Microsoft Server 2003 and Oracle Linux Server, the FABS application (Oracle Web Logic) and database (Oracle 10g) servers reside on the FLETC GAN in a Hybrid physical network topology and are accessible from four sites: Georgia (GA), DC, New Mexico, and Maryland. The system owner and responsible office is the Finance Division Chief in the FLETC OCFO.

Glynco Administrative Network (GAN)

The purpose of GAN is to provide access to IT network applications and services to include video and voice teleconferencing to authorized FLETC personnel, contractors and partner organizations located at the Georgia facility. It provides authorized users access to email, internet services, required applications such as Financial Management Systems, Procurement systems, Property management systems, Video conference, and other network services and shared resources. The GAN is located in GA and is owned and operated by the FLETC OCIO.

Appendix B

FY 2013 IT Notices of Findings and Recommendations at FLETC and I&A/OPS

Department of Homeland Security
Information Technology Management Letter
Federal Law Enforcement Training Center
September 30, 2013

FY 2013 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FLETC-IT-13-01	FLETC Momentum Audit Log Reviews not Consistently Maintained	Access Controls	X	
FLETC-IT-13-02	Weakness in GAN Password Complexity	Access Controls	X	
FLETC-IT-13-03	FLETC Momentum Account Management not Consistently Performed	Access Controls	X	
FLETC-IT-13-04	Momentum Application Inactivity Lockout is not Appropriately Configured	Access Controls	X	
FLETC-IT-13-05	FLETC Contractor Separation not Fully Monitored	Access Controls	X	
IAOPS-IT-13-01	IA&OPS Momentum Audit Log Reviews not Consistently Performed in a Timely Manner	Access Controls	X	
IAOPS-IT-13-02	IA&OPS Segregation of Duties not Fully Enforced	Segregation of Duties	X	
IAOPS-IT-13-03	IA&OPS Momentum Account Management not Consistently Performed	Access Controls		X
IAOPS-IT-13-04	Momentum Application Inactivity Lockout is not Appropriately Configured	Access Controls	X	
IAOPS-IT-13-05	IA&OPS Contractor Separation not Fully Monitored	Access Controls	X	
IAOPS-IT-13-06	Multiple Payment Vouchers can be Processed Against the Same Invoice	Business Process Controls	X	

Appendix A
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy 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 Financial Officer
Chief Information Officer
Chief Information Security Officer
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION

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 (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Office of Investigations Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

The OIG seeks to protect the identity of each writer and caller.