Department of Homeland Security

Office of Inspector General

Information Technology Management Letter for the Federal Law Enforcement Training Center Component of the FY 2012 Department of Homeland Security Financial Statement Audit

OIG-13-62

April 2013

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

April 4, 2013

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

Alan Titus
Chief Financial Officer
Federal Law Enforcement Training Center

FROM: Frank Deffer
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the Federal Law Enforcement Training Center Component of the FY 2012 Department of Homeland Security Financial Statement Audit*

Attached for your action is our final report, *Information Technology Management Letter for the Federal Law Enforcement Training Center Component of the FY 2012 Department of Homeland Security Financial Statement Audit.* The independent accounting firm KPMG LLP (KPMG) performed the audit of DHS' financial statements as of September 30, 2012, and prepared this information technology (IT) management letter.

KPMG is responsible for the attached IT management letter dated December 12, 2012, and the conclusion expressed in it. We do not express an opinion on DHS' financial statements or internal controls or conclusions on compliance with laws and regulations. The DHS management concurred with all recommendations.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

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

April 3, 2013

Inspector General
U.S. Department of Homeland Security

Chief Information Officer and
Chief Financial Officer
Federal Law Enforcement Training Center

We have audited the balance sheet of the U.S. Department of Homeland Security (DHS or Department) as of September 30, 2012, and the related statements of net cost, changes in net position, and custodial activity, and combined statement of budgetary resources for the year then ended (referred to as the "fiscal year (FY) 2012 financial statements"). We were also engaged to audit the Department's internal control over financial reporting of the FY 2012 financial statements. The objective of our audit engagement was to express an opinion on the fair presentation of the FY 2012 financial statements and the effectiveness of internal control over financial reporting of the FY 2012 financial statements.

In accordance with *Government Auditing Standards*, our *Independent Auditors' Report*, dated November 14, 2012, included internal control deficiencies identified during our audit engagement 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).

During our audit engagement, we noted certain matters in the areas of access controls, configuration management, and segregation of duties with respect to FLETC' financial systems general information technology controls (GITC). These matters are described in the *General IT Control Findings and Recommendations* section of this letter.

The comments described herein have been discussed with the appropriate members of management, or communicated through a Notice of Finding and Recommendation (NFR), and are intended For Official Use Only. We aim to use our knowledge of DHS' organization gained during our audit engagement to make comments and suggestions that we hope will be useful to you. We have not considered internal control since the date of our *Independent Auditors' Report*.

The Table of Contents on the next page identifies each section of the letter. We have provided a description of key FLETC financial systems within the scope of the FY 2012 DHS financial statement audit engagement in Appendix A; a description of each internal control finding in Appendix B; and the current status of the prior year NFRs in Appendix C. Our comments related to financial management and reporting internal controls (comments not related to IT) have been presented in a separate letter to the Office of Inspector General (OIG) and the DHS Chief Financial Officer.

This report is intended solely for the information and use of DHS management, DHS OIG, U.S. Office of Management and Budget, U.S. Government Accountability Office (GAO), and the U.S. Congress, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE, AND APPROACH

In connection with our engagement to audit the financial statements of DHS as of and for the year ended September 30, 2012, we performed an evaluation of general Information Technology (IT) controls (GITCs) at FLETC and I&A/Ops, to assist in planning and performing our audit engagement. FLETC provides financial management services to I&A/Ops and hosts a separate Momentum environment, which was developed to mirror the FLETC Momentum environment. The *Federal Information System Controls Audit Manual* (FISCAM), issued by the GAO, formed the basis of our GITC evaluation procedures. The scope of the GITC evaluation is further described in Appendix A.

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 functions to be essential to the effective operation of GITCs and the IT environment.

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

- *Configuration Management (CM)* – Controls that help to prevent unauthorized changes to information system resources (software programs and hardware configurations) and provides reasonable assurance that systems are configured and operating securely and as intended.

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

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

To complement our GITC audit procedures, we conducted a review over the FLETC's technical security testing for key network and system devices, and performed testing over key financial application controls in the FLETC environment.

In addition to testing FLETC's general control environment, we performed application control tests on a limited number of FLETC's financial systems and applications. The application control testing was performed to assess the controls that support the financial systems' internal controls over the input, processing, and output of financial data and transactions.

- *Application Controls (APC)* - Application controls are the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, or payroll.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During FY 2012, FLETC took corrective action to address one of the IT control weaknesses from the prior year. FLETC decommissioned the Student Information System, which was previously in the scope of the financial audit. However, during FY 2012, we identified IT general control weaknesses that could potentially impact FLETC's financial data.

FLETC provides financial management services to I&A/Ops and hosts a separate Momentum environment, which was developed to mirror the FLETC Momentum environment. However, we found that the most significant findings from a financial statement audit perspective were related to the I&A/Ops Momentum database access control and configuration management. In addition, we noted that after several years of improved processes over technical security testing, FLETC has inadequate patch management over servers and workstations. Collectively, the IT control deficiencies limited FLETC's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability.

Of the 4 findings identified during our FY 2012 testing; 3 were new IT findings. These findings represent control deficiencies in three of the five FISCAM key control areas: configuration management, access controls, and segregation of duties. Specifically, these control deficiencies include the need for:

1. Better designed and operating configuration management;
2. Effective segregation of duties controls within a financial application;
3. Patch management; and
4. Stronger account management.

These control deficiencies may increase the risk that the confidentiality, integrity, and availability of system controls and FLETC financial data could be exploited thereby compromising the integrity of financial data used by management as reported in DHS' consolidated financial statements. While the recommendations made by KPMG should be considered by FLETC, it is the ultimate responsibility of FLETC management to determine the most appropriate method(s) for addressing the weaknesses identified based on their system capabilities and available resources.

GENERAL IT CONTROL FINDINGS AND RECOMMENDATIONS

FLETC

Findings:

During our engagement to audit the FY 2012 DHS financial statements, we identified the following FLETC GITC control deficiencies.

Access Controls

- Security patch management deficiencies were identified during the vulnerability assessment on the platforms supporting the key financial applications and general support systems.

Segregation of Duties

- Procedures to enforce least privilege and segregation of duties to Momentum were not effectively managed.

Recommendations:

We recommend that the FLETC Chief Information Officer (CIO) and Chief Financial Officer (CFO), in coordination with the DHS Office of Chief Financial Officer (OCFO) and the DHS Office of the Chief Information Officer (OCIO), make the following improvements to FLETC's financial management systems and associated information technology security program.

For Access Controls

- Enforce existing vulnerability management procedures which require updating security patches in a timely manner.

For Segregation of Duties

- Enforce policies and procedures to ensure that assigned roles and responsibilities are commensurate with personnel job functions.

I&A/Ops

Findings:

During our engagement to audit the FY 2012 DHS financial statements, we identified the following I&A/Ops IT and financial system control deficiencies that, while they were not a contributing factor to the material weaknesses at the Department level, need improvement.

Configuration Management

- Evidence to support that Momentum I&A/Ops system changes were approved and tested prior to movement into the production environment was not maintained.

Access Controls

- Access controls within the I&A/Ops Momentum environment were not effectively managed:
  - User access was not consistently provisioned in accordance with "least privilege" principles; specifically, two I&A/Ops employees had access privileges in excess of VIEW;
  - Profile change approvals were not consistently documented; specifically, one of two users selected had his or her access privileges modified without having formally documented approval;
  - User access was not consistently revoked upon employee termination; specifically, two FLETC personnel retained active I&A/Ops Momentum access following their separation; and,
  - User access was not recertified.

Recommendations:

We recommend that the FLETC CIO and CFO, in coordination with the DHS OCFO and the DHS OCIO**,** make the following improvements to FLETC's financial management systems and associated information technology security program.

For Configuration Management

- Develop and implement policies and procedures to approve and test I&A/Ops Momentum changes prior to movement into the production environment.

For Access Controls

- Develop and implement policies and procedures to formalize access management and user profile monitoring for the Momentum I&A/Ops environment.

APPLICATION CONTROLS

We did not identify any findings in the area of application controls during the fiscal year 2012 FLETC audit engagement.

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2012

Appendix A

Description of Key FLETC and I&A/Ops Financial Systems and IT Infrastructure within the Scope of the FY 2012 DHS Financial Statement Audit

Below is a description of significant FLETC financial management systems and supporting IT infrastructure included in the scope of FLETC's FY 2012 financial statement audit.

Financial Accounting and Budgeting System (FABS)

The FLETC FABS application 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 and hosts a separate 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. An application called "Tuxedo," also resides on a separate server. The Tuxedo middleware holds 67 executable files. These files are scripts that process daily information and are not directly accessible by users. The FABS application and servers reside on the FLETC Local Area Network in a Hybrid physical network topology and are accessible from four sites: Georgia (GA), Washington DC, New Mexico, and Maryland.

Glynco Administrative Network (GAN)

The purpose of the GAN is to provide access to IT network applications and services to include voice 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.

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2012

Appendix B

FY 2012 Notices of IT Findings and Recommendations at FLETC and I&A/Ops

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2012

FY 2011 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FLETC-IT-12-01	Ineffective Segregation of Duties Controls for the Momentum System	Segregation of Duties		X
FLETC-IT-12-02	FLETC Servers and Workstations have Inadequate Patch Management	Configuration Management	X	
MGA-IT-12-03	I&A/Ops Momentum Access Controls are not Consistently Applied	Access Controls	X	
MGA-IT-12-04	Configuration Changes for the I&A/Ops Momentum System are not Consistently Documented	Configuration Management	X	

Appendix C

Status of Prior Year Notices of Findings and Recommendations and Comparison to Current Year Notices of Findings and Recommendations (at FLETC only)

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2012

NFR #	Description	Disposition	
		Closed	Repeat
FLETC-IT-11-01	Ineffective Logical Access Controls over the GAN	X	
FLETC-IT-11-02	Ineffective Segregation of Duties controls for the Momentum System		X

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

For additional information, visit our website at: www.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: DHS Office of Inspector General, Attention: Office of Investigations Hotline, 245 Murray Drive, SW, Building 410/Mail Stop 2600, Washington, DC, 20528; or you may call 1 (800) 323-8603; or fax it directly to us at (202) 254-4297.

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