

**Information Technology
Management Letter for the
Federal Law Enforcement
Center Component of the
FY 2015 Department of
Homeland Security Financial
Statement Audit**





DHS OIG HIGHLIGHTS

Information Technology Management Letter for the Federal Law Enforcement Center Component of the FY 2015 Department of Homeland Security Financial Statement Audit

April 1, 2016

Why We Did This

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 FLETC, 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

What We Found

We contracted with the independent public accounting firm KPMG, LLP to perform the audit the consolidated financial statements of the U.S. Department of Homeland Security for the year ended September 30, 2015. KPMG evaluated select general information technology controls (GITCs), entity level controls, and business process application controls at the Federal Law Enforcement Training Center (FLETC). KPMG determined that FLETC took corrective action to address certain prior IT control deficiencies. For example, FLETC made improvements by designing and consistently implementing controls related to the separation and termination of contractors.

However, KPMG continued to identify GITC deficiencies related to access controls and configuration management for FLETC's core financial systems. The conditions supporting our findings collectively limited FLETC's ability to ensure that critical financial and operational data were maintained in such a manner as to ensure their confidentiality, integrity, and availability.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

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

April 1, 2016

MEMORANDUM FOR: 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 Center 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 Federal Law Enforcement Center 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 Audit 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,
Federal Law Enforcement Training Centers
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 the Federal Law Enforcement Training Centers (FLETC), 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.

With respect to financial systems at FLETC, we noted certain internal control deficiencies in the general information technology (IT) control area 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 FLETC financial systems and IT infrastructure within the scope of the FY 2015 DHS financial statement audit in Appendix A, and a listing of each FLETC 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 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 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 the FLETC 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 Centers
September 30, 2015

TABLE OF CONTENTS

	Page
Objective, Scope, and Approach	2
Summary of Findings	4
Findings and Recommendations	5
Findings	5
Recommendations	5

APPENDICES

Appendix	Subject	Page
A	Description of Key FLETC Financial Systems and IT Infrastructure within the Scope of the FY 2015 DHS Financial Statement Audit	7
B	FY 2015 IT Notices of Findings and Recommendations at FLETC	9

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, 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 Federal Law Enforcement Training Centers (FLETC), 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 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 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
Federal Law Enforcement Training Centers
September 30, 2015

information provided by the entity in support of our financial audit procedures. Consequently, FY 2015 GITC procedures at FLETC 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 FLETC'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. Some key financial feeder systems are not fully integrated with the main financial system. Therefore, in FY 2015 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 financial systems and IT infrastructure within the scope of the FY 2015 DHS financial statement audit.

Department of Homeland Security
Information Technology Management Letter
Federal Law Enforcement Training Centers
September 30, 2015

SUMMARY OF FINDINGS

During FY 2015, 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 separation and termination of contractors. However, we continued to identify GITC deficiencies related to access controls and configuration management for FLETC's core financial systems.

The conditions supporting our findings collectively limited FLETC's ability to ensure that critical financial and operational data were maintained in such a manner as to ensure confidentiality, integrity, and availability. Of the four IT Notices of Findings and Recommendations (NFRs) issued during our FY 2015 testing at FLETC, all were new findings.

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 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 financial applications.

During our IT audit procedures, we also evaluated and considered the impact of financial system functionality on financial reporting.

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

FINDINGS AND RECOMMENDATIONS

Findings

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

Access Controls

- Strong password requirements were not consistently enforced on databases supporting the financial application.
- Controls to ensure that users with access to the operating system supporting the financial application are removed in a timely manner when access is no longer needed were inadequate.
- Documentation supporting account management activities, including recertification of database accounts that support the financial application, was not consistently maintained in accordance with established procedures.

Configuration Management

- Certain configuration-related deficiencies identified on servers and system software were not remediated within a timely manner and tracked appropriately for remediation within management's Plan of Action and Milestone (POA&M).

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 financial management systems and associated IT security program (in accordance with FLETC and DHS requirements, as applicable):

Access Controls

- Conduct a risk assessment and cost-benefit analysis of implementing strong passwords to be in compliance with DHS guidelines, and submit a waiver for non-compliance until this remediation is complete.
- Enforce access controls and provide user account information to the appropriate individuals to ensure accuracy and recertify the users.
- Implement an automated process to send email notifications to the database administrator and system owner to review user accounts every 90 days and maintain evidence of this process.

Department of Homeland Security
Information Technology Management Letter
Federal Law Enforcement Training Centers
September 30, 2015

Configuration Management

- Improve the current vulnerability management process to include timely creation of POA&Ms that cannot be addressed within the existing patch management cycle.

Appendix A

Description of Key FLETC Financial Systems and IT Infrastructure within the Scope of the FY 2015 DHS Financial Statement Audit

Department of Homeland Security
Information Technology Management Letter
Federal Law Enforcement Training Centers
September 30, 2015

Below is a description of the significant FLETC financial management system and supporting IT infrastructure included in the scope of the FY 2015 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. An instance of the commercial off-the-shelf (COTS) financial processing system known as Momentum, it 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 U.S. Department of Agriculture's (USDA) National Finance Center (NFC) and the General Services Administration's Concur Government Edition (CGE) electronic travel system.

The application is supported by an Oracle database with Microsoft Windows-based and Red Hat UNIX-based servers.

FABS is physically hosted within Datacenter 1, in Stennis, Mississippi, and managed by a service provider who performs operating system administration. FLETC still performs database and application administration.

Purchase Request Information System (PRISM)

PRISM is a contract writing system used by FLETC acquisition personnel to create contract awards. PRISM is interfaced with the Federal Procurement Data System – Next Generation. FLETC utilizes an instance of the application while the DHS Office of the Chief Procurement Officer (OCPO) owns and manages the system. OCPO is responsible for application configuration, operating system and database administration.

PRISM is supported by an Oracle database with UNIX-based servers. The system resides in Datacenter 1, in Stennis, Mississippi.

Web Time and Attendance (WebTA)

WebTA is a COTS web-based major application hosted by the USDA's NFC and developed, operated, and maintained by the NFC IT Services Division and NFC Risk Management Staff. DHS components utilize NFC and WebTA to process the front-end input and certification of time and attendance entries by the DHS user community to facilitate payroll processing.

EmpowHR

EmpowHR is a COTS web-based major application hosted by the NFC and developed, operated, and maintained by the NFC IT services division and NFC Risk Management Staff. DHS components utilize NFC and EmpowHR to initiate, authorize, and send personnel data to NFC for processing.

Department of Homeland Security
Information Technology Management Letter
Federal Law Enforcement Training Centers
September 30, 2015

Appendix B
FY 2015 IT Notices of Findings and Recommendations at FLETC

Department of Homeland Security
Information Technology Management Letter
Federal Law Enforcement Training Centers
September 30, 2015

FY 2015 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FLETC-IT-15-01	Weakness in Momentum Database Security Configurations	Access Controls	X	
FLETC-IT-15-02	Inappropriate Access to the FABS Operating System	Access Controls	X	
FLETC-IT-15-03	Weakness in FABS Database Account Recertification	Access Controls	X	
FLETC-IT-15-04	Security Management and Configuration Management Controls-Vulnerability Assessment	Configuration Management	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

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