

**Information Technology
Management Letter for
the Federal Law
Enforcement Training
Centers Component of
the FY 2016 Department
of Homeland Security
Financial Statement
Audit**





DHS OIG HIGHLIGHTS

Information Technology Management Letter for the Federal Law Enforcement Training Centers Component of the FY 2016 Department of Homeland Security Financial Statement Audit

June 26, 2017

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) 2016 DHS Agency Financial Report.

What We Recommend

We recommend that FLETC, in coordination with the DHS Chief Information Officer and Acting 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 of the consolidated financial statements of the U.S. Department of Homeland Security (DHS) for the year ended September 30, 2016. KPMG evaluated selected general IT controls (GITC) and business process application controls at the Federal Law Enforcement Training Centers (FLETC). KPMG determined that FLETC took corrective action to address certain prior-year IT control deficiencies. For example, FLETC made improvements in account management activities related to the database and operating system. However, KPMG continued to identify GITC deficiencies related to access controls and configuration management for FLETC's core financial systems.

The deficiencies 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. In addition, certain of these deficiencies adversely impacted internal controls over DHS' financial reporting and its operation and therefore are considered to collectively represent a material weakness reported in the FY 2016 DHS Agency Financial Report.



OFFICE OF INSPECTOR GENERAL

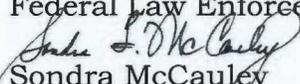
Department of Homeland Security

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

June 26, 2017

MEMORANDUM FOR: Michael Vesta
Acting Chief Information Officer
Federal Law Enforcement Training Centers

Donald Lewis
Chief Financial Officer
Federal Law Enforcement Training Centers

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

SUBJECT: *Information Technology Management Letter for the
Federal Law Enforcement Training Centers Component of
the FY 2016 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 Centers Component of the FY 2016 Department of Homeland Security Financial Statement Audit*. This report contains comments and recommendations related to information technology internal control deficiencies. The deficiencies did not meet the criteria to be reported in the *Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting*, dated November 14, 2016, which was included in the FY 2016 DHS Agency Financial Report.

The independent public accounting firm KPMG, LLP conducted the audit of DHS' FY 2016 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 Kevin Burke, Acting Director, Information Systems and Acquisitions Division, at (202) 254-5450.

Attachment



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

December 15, 2016

Office of Inspector General
U.S. Department of Homeland Security
Washington, DC

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

Ladies and Gentlemen:

We planned and performed 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, 2016, 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.

We also noted certain internal control deficiencies at FLETC during our audit that, in aggregate and when combined with certain internal control deficiencies identified at certain other DHS components, contributed to a material weakness in information technology (IT) controls and financial system functionality at the DHS Department-wide level. Specifically, with respect to financial systems at FLETC, we noted certain matters in the general IT control areas 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 Fiscal Year (FY) 2016 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, 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 DHS Office of Inspector General (OIG) and the FLETC Chief Financial Officer.



Our audit procedures are designed primarily to enable us to form opinions on the FY 2016 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.

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, 2016

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 2016 DHS Financial Statement Audit	7
B	FY 2016 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, 2016, (referred to herein as the “fiscal year (FY) 2016 financial statements”). In connection with our audit of the FY 2016 DHS consolidated financial statements, we performed an evaluation of selected general information technology (IT) controls (GITC) 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 U.S. Government Accountability Office (GAO) issued the *Federal Information System Controls Audit Manual* (FISCAM), which 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. It 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.

Although 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 information provided by the entity in support of our financial audit procedures. Consequently, FY 2016 GITC procedures evaluated at FLETC did not necessarily represent controls from each FISCAM category.

Department of Homeland Security
Information Technology Management Letter
Federal Law Enforcement Training Centers
September 30, 2016

Business Process Application Controls

Where relevant GITCs were operating effectively, we tested selected IT application controls (process-level controls — fully automated or manual with an automated component) on financial systems and applications to assess internal controls over input, processing, and output of financial data and transactions.

FISCAM defines Business Process Application Controls (BPAC) 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. BPACs 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. Many key financial and feeder systems have not been substantially updated since being inherited from legacy agencies several years ago. Therefore, in FY 2016, 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 2016 DHS financial statement audit.

SUMMARY OF FINDINGS

During our FY 2016 assessment of GITCs and IT application controls, we noted that FLETC took corrective action to address certain prior year IT control deficiencies. For example, FLETC made improvements in account management activities related to the database and operating system. 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 their confidentiality, integrity, and availability. In addition, certain of these deficiencies at FLETC adversely impacted the internal controls over DHS' financial reporting and its operation and we consider them to collectively contribute to a Department-wide material weakness regarding IT controls and financial system functionality for DHS, under standards established by the American Institute of Certified Public Accountants and the U.S. GAO.

Of the four IT Notices of Findings and Recommendations (NFR) issued during FY 2016 testing at FLETC, two were repeat findings, either wholly or in part from the prior year, and two were new findings. The four IT NFRs issued represent deficiencies and observations related to two of the five FISCAM GITC categories.

The majority of the deficiencies that our audit identified were related to noncompliance with financial system controls. According to DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program*; National Institute of Standards and Technology guidance; and FLETC policies; financial system controls lacked proper documentation, were not fully designed and implemented, were inadequately detailed, and were inconsistently implemented. The most significant weaknesses from a financial statement audit perspective included insufficient controls regarding audit logs and database passwords.

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

Although the recommendations made by us should be considered by FLETC, it is ultimately the 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 2016 DHS consolidated financial statements, we identified the following GITC deficiencies at FLETC, certain of which, in the aggregate, contribute to the IT material weakness at the Department level:

Access Controls

- Strong password requirements were not consistently enforced on databases supporting the financial application.
- Requirements for generating audit logs, with the detail needed to review application-level auditable events, had not been implemented for the database and operating system.
- Privileged users on databases supporting the key financial application were not uniquely identified and shared user IDs and passwords.

Configuration Management

- Certain configuration-related deficiencies identified on servers and system software were not remediated timely and tracked appropriately within management's Plan of Action and Milestones (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

- Submit a waiver for non-compliance of database passwords along with the formal risk assessment and update password configuration on the default profile.
- Expand audit log reviews to cover sufficient detail to facilitate reconstruction of events and ensure that audit logs are reviewed as specified in the System Security Plan (SSP).
- Improve oversight of the database administrator functions and provide adequate training on security best practices.

Department of Homeland Security
Information Technology Management Letter
Federal Law Enforcement Training Centers
September 30, 2016

Configuration Management

- Improve the current vulnerability management procedures to ensure that identified weaknesses are documented and remediated in a timely manner.

Department of Homeland Security
Information Technology Management Letter
Federal Law Enforcement Training Centers
September 30, 2016

Appendix A

**Description of Key FLETC Financial Systems and IT Infrastructure within the Scope of the FY 2016
DHS Financial Statement Audit**

Department of Homeland Security
Information Technology Management Letter
Federal Law Enforcement Training Centers
September 30, 2016

Below is a description of the significant FLETC financial management systems and supporting IT infrastructure included in the scope of the FY 2016 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. FABS is a commercial off-the-shelf (COTS) financial processing system known as Momentum, and 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 the systems of 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 electronic travel system.

An Oracle database with Microsoft Windows-based and Red Hat UNIX-based servers supports the application.

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

Procurement Request Information System Management (PRISM)

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

An Oracle database with UNIX-based servers supports PRISM. The system resides in Datacenter 1 in Stennis, MS.

Web Time and Attendance (WebTA)

WebTA is a COTS web-based major application that the USDA NFC hosts. The NFC's IT Services Division and Risk Management Staff developed, operate, and maintain it. FLETC uses WebTA to process front-end input and certification of time and attendance entries by the FLETC user community to facilitate payroll processing.

EmpowHR

EmpowHR is a COTS web-based major application that NFC hosts. NFC's IT Services Division and Risk Management Staff developed, operate, and maintain it. DHS components use 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, 2016

Appendix B

FY 2016 IT Notices of Findings and Recommendations at FLETC

Department of Homeland Security
Information Technology Management Letter
Federal Law Enforcement Training Centers
September 30, 2016

FY 2016 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FLETC-IT-16-01	Non-Compliance with Baseline Configuration Guidance for Oracle Database User Account Passwords	Access Controls		X
FLETC-IT-16-02	Insufficient Audit Log Controls for Key Financial Systems	Access Controls	X	
FLETC-IT-16-03	Excessive Non-Unique Database Access Privileges	Access Controls	X	
FLETC-IT-16-04	Weaknesses Identified Through Vulnerability Assessment Procedures on Financially Significant Environments Hosted at DC1	Configuration Management		X



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

Management Directorate

Acting Chief Financial Officer
Chief Information Officer
Audit Liaison

Federal Law Enforcement Training Centers

Director
Chief Financial Officer
Acting 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