Department of Homeland Security
Office of Inspector General

Information Technology Management Letter for the Federal Law Enforcement Training Center Component of the FY 2010 DHS Financial Statement Audit

OIG-11-76

April 2011

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 25028

Homeland Security

APR 20 2011

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report presents the information technology (IT) management letter for the FY 2010 Federal Law Enforcement Training Center (FLETC) component of the DHS financial statement audit as of September 30, 2010. It contains observations and recommendations related to information technology internal control that were summarized in the *Independent Auditor's Report* dated November 12, 2010 and presents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit procedures at the FLETC component in support of the DHS FY 2010 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated March 18, 2011, and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control or conclusion on compliance with laws and regulations.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Frank Deffer
Assistant Inspector General
Information Technology Audits

KPMG LLP
2001 M Street, NW
Washington, DC 20036-3389

March 18, 2011

Inspector General
U.S. Department of Homeland Security

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

Ladies and Gentlemen:

We were engaged to audit the balance sheet of the U.S. Department of Homeland Security (DHS or Department), as of September 30, 2010 and the related statement of custodial activity for the year then ended (herein after referred to as "financial statements"). We were also engaged to examine the Department's internal control over financial reporting of the balance sheet as of September 30, 2010 and the statement of custodial activity for the year then ended. We were not engaged to audit the statements of net cost, changes in net position, and budgetary resources as of September 30, 2010 (hereinafter referred to as "other fiscal year (FY) 2010 financial statements"), or to examine internal control over financial reporting over the other FY 2010 financial statements.

Because of matters discussed in our *Independent Auditors' Report,* dated November 12, 2010, the scope of our work was not sufficient to enable us to express, and we did not express, an opinion on the financial statements or on the effectiveness of DHS' internal control over financial reporting of the balance sheet as of September 30, 2010, and related statement of custodial activity for the year then ended. Additional deficiencies in internal control over financial reporting, potentially including additional material weaknesses and significant deficiencies, may have been identified and reported had we been able to perform all procedures necessary to express an opinion on the financial statements or on the effectiveness of DHS' internal control over financial reporting of the balance sheet as of September 30, 2010, and related statement of custodial activity for the year then ended; and had we been engaged to audit the other FY 2010 financial statements, and to examine internal control over financial reporting over the other FY 2010 financial statements.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

The Federal Law Enforcement Training Center (FLETC) is a component of DHS. During our audit engagement, we noted certain matters in the areas of information technology (IT) configuration management, access controls, and security management with respect to FLETC's financial systems information technology (IT) general controls, which we believe contribute to an IT material weakness at the DHS level. These matters are described in the *IT General Control Findings and Recommendations* section of this letter.

The material weakness described above is presented in our *Independent Auditors' Report*, dated November 12, 2010. This letter represents the separate limited distribution letter mentioned in that report.

The control deficiencies described herein have been discussed with the appropriate members of management, and communicated through a Notice of Finding and Recommendation (NFR).

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate. We aim to use our knowledge of FLETC gained during our audit engagement to make comments and suggestions that are intended to improve internal control over financial reporting or result in other operating efficiencies. 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 and IT infrastructure within the scope of our engagement to audit the FY 2010 DHS financial statements in Appendix A; a listing of the FY 2010 IT Notices of Findings and Recommendations (NFR) at FLETC in Appendix B; and the status of the prior year NFRs and a comparison to current year NFRs at FLETC in Appendix C. Our comments related to certain additional matters have been presented in a separate letter to the Office of Inspector General and the FLETC Chief Financial Officer.

FLETC's written response to our comments and recommendations has not been subjected to auditing procedures and, accordingly, we express no opinion on it.

This communication is intended solely for the information and use of DHS and FLETC management, DHS Office of Inspector General, Office of Management and Budget (OMB), U.S. Government Accountability Office, 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

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2010

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE AND APPROACH

In connection with our engagement to audit DHS' balance sheet as of September 30, 2010 and the related statement of custodial activity for the year then ended, we performed an evaluation of the information technology general controls (ITGC), at FLETC to assist in planning and performing our audit. The *Federal Information System Controls Audit Manual* (FISCAM), issued by GAO, formed the basis of our ITGC evaluation procedures. The scope of the ITGC evaluation is further described in Appendix A.

FISCAM was designed to inform financial 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 audit. FISCAM also provides guidance to IT auditors when considering the scope and extent of review that generally should be performed when evaluating general controls and the IT environment of a federal agency. FISCAM defines the following five control functions to be essential to the effective operation of the general IT controls 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 general IT controls audit procedures, we also performed technical security testing for key network and system devices. The technical security testing was performed both over the Internet and from within select FLETC facilities, and focused on test, development, and production devices that directly support key general support systems.

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 2010, FLETC took corrective action to address prior year IT control weaknesses. For example, FLETC made improvements over configuration management in Momentum and the Glynco Area Network (GAN) and management review over Momentum auditing logs. However, during FY 2010, we continued to identify IT general control weaknesses that could potentially impact FLETC's financial data. The most significant weaknesses from a financial statement audit perspective were related to the GAN logical access controls and weaknesses over physical security and security awareness. Collectively, the IT control weaknesses limited FLETC's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively impacted the internal controls over FLETC financial reporting and its operation and contribute to a material weakness at the department level under standards established by the American Institute of Certified Public Accountants. In addition, based upon the results of our test work, we noted that FLETC did not fully comply with the requirements of the *Federal Financial Management Improvement Act* (FFMIA).

Of the six findings identified during our FY 2010 testing, one was a new IT finding. These findings represent control deficiencies in three of the five FISCAM key control areas. The FISCAM areas impacted include configuration management, security management, and access controls. The specific weakness were 1) lack of management and review of system audit logs, 2) ineffective account management issues involving user profiles, and account lockout, and 3) inadequately trained personnel on basic security management policies and procedures. 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.

IT GENERAL CONTROL FINDINGS AND RECOMMENDATIONS

Findings:

During the FY 2010 DHS financial statement audit, we identified the following IT and financial system control deficiencies at FLETC that in the aggregate contribute to the IT material weakness at the Department level.

Configuration Management

- Momentum and GAN changes are not being documented throughout the change control process from the testing of changes to the final approval of the changes prior to implementation, and;
- Distribution and implementation of Momentum and GAN changes are not being controlled.

Access Control

- Weak logical access controls over the GAN were noted as follows:
    - The GAN resets the account failed logon counter after 20 minutes, which does not meet the DHS 4300A requirement of 24 hours. Upon notification, FLETC immediately remediated the configuration issue, therefore, no recommendation will be offered for this issue.
- GAN security violation audit logs lack management review and signoff.
- Momentum user profile creation or modification is not logged or tracked.
- Weak logical access controls over the Student Information System (SIS) were noted as follows:
    - Password length is configured to a minimum of 6, which does not meet the DHS 4300A requirement of 8.
    - SIS is not configured to reset the account failed logon counter, which does not meet the DHS 4300A requirement of a reset every 24 hours.
    - User lockout occurs after 6 invalid attempts (only 3 attempts permitted per DHS 4300A).
    - A sample of audit logs that track changes to system data could not be provided.
    - User profile creation is not tracked and a listing of profile creation dates could not be provided.
    - Periodic review of user accounts is not being performed.

Security Management

We performed after-hours physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects included physical access to media and equipment that housed financial data and information residing within a FLETC employee's or contractor's work area, which could be used by others to gain unauthorized access to systems housing financial information. The

testing was performed at various FLETC locations that process and/or maintain financial data. The specific results are listed as shown in the following table:

Exceptions Noted	FLETC Locations Tested				Total Exceptions by Type
	IT Office, Building 681	Finance Office, Building 66	Procurement, and SIS, Building 93	Telecommunications Facility, Building 94	
User Name and Passwords	1	3	0	0	**4**
For Official Use Only (FOUO)	0	0	0	0	**0**
Keys/Badges	0	0	0	0	**0**
Personally Identifiable Information (PII)	0	8*	0	0	**8**
Server Names/IP Addresses	2	0	0	0	**2**
Laptops	0	0	0	0	**0**
External Drives	0	0	0	0	**0**
Credit Cards	0	1	0	0	**1**
Classified Documents	0	0	0	0	**0**
Other - Describe	2 workstations logged in w\o screensaver activated	0	0	0	**2**
Total Exceptions by Location	**5**	**12**	**0**	**0**	**17**

*37 boxes of PII (names, birth date, address, SS#). Counted as one incident

Recommendations:

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

Configuration Management

We recommend that FLETC management update and enforce current procedures to ensure changes are fully documented throughout the change control process to include the results of testing the change, review of the change test results, and final approval to proceed with the implementation.

Access Control

- Continue with the procurement and deployment of ArcSight Enterprise Security Management (ESM) as a replacement Security Information Management (SIM) solution for audit logging.
- Develop a Standard Operating Procedure (SOP) to implement management oversight for Momentum access authorizations for user's profiles created or modified during the fiscal year.
- Configure or enhance existing automated controls to meet DHS requirements in financial systems. Alternatively, adequate mitigating controls may be relied upon to assure financial data is protected.

Security Management

We recommend that FLETC continue the physical controls enhancements in the Finance Division, Building 66. In addition, develop a Standard Operating Procedure (SOP) to address Safeguarding of PII and Credit Card data in the Finance Division, implement use of the secure file storage rooms, and address entry controls for access points in the building.

APPLICATION CONTROLS

We did not identify any findings in the area of application controls during the fiscal year 2010 FLETC audit engagement.

MANAGEMENT'S COMMENTS AND OIG RESPONSE

We obtained written comments on a draft of this report from FLETC's Chief Information Officer. Generally, FLETC management agreed with our findings and recommendations. FLETC management has developed a remediation plan to address these findings and recommendations. A copy of the comments is included in Appendix D.

OIG Response

We agree with the steps that FLETC management is taking to satisfy these recommendations.

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2010

Appendix A

Description of Key FLETC Financial Systems and IT Infrastructure within the Scope of the FY 2010 DHS Financial Statement Audit

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2010

Below is a description of significant FLETC financial management systems and supporting IT infrastructure included in the scope of the DHS Financial Statement Audit.

Financial Accounting and Budgeting System (FABS)

- Processing Location*:* FLETC Headquarters in Glynco, GA

General System Description:

The FLETC FABS application is an all-in-one financial processing system. It functions as the computerized accounting and budgeting system for FLETC. The FABS system exists to provide all of the financial and budgeting transactions in which FLETC is involved. The FABS environment primarily consists of the latest version of the Momentum version 6.1 COTS software, an Oracle 10g database and its companion Oracle 10.2 Database Management System (DBMS). 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 LAN in a Hybrid physical network topology and are accessible from four sites: Glynco, GA, Washington D.C., Artesia, New Mexico, and Cheltenham, MD.

- Hardware: Hewlett Packard ProLiant BL465c Blade Servers (web and application) and Hewlett Packard ProLiant BL685c Blade Servers (database)
- Operating System: Microsoft Windows 2003 Server running on virtual machines on top of VMware Infrastructure 3.5 Enterprise hypervisor on the web and application servers
- Database: Red Hat Enterprise Linux
- Security Software: FABS system does not currently have a firewall scheme and resides on FLETC LAN that has a firewall in place

Interfaces:

- National Finance Center (NFC) Payroll System
- Student Information System
- Treasury Information Executive Repository (TIER)
- US Coast Guard Interface
- Kansas City Financial Center (KFC)

Glynco Administrative Network

- Processing Location*:* FLETC Headquarters in Glynco, GA

General System Description:

The purpose of 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 Glynco, Georgia facility. It provides authorized users access to email, internet services, required applications such as Financial Management Systems (FMS), Procurement systems, Property management systems, Video conferencing, and other network services and shared resources.

- Hardware: Cisco ACS TACAS Server, Avaya 8700 Media Servers, Dell Poweredge servers 1750, 1850, 1950, 2650, 2850, 2950, and 6650.
- Operating System: Windows XP SP2 (Desktop)

- Database: Redhat Linux 4 Enterprise edition
- Security Software: ASA 5500 series firewall and static IP addresses

Interfaces:

- FMS
- DHS HQ

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2010

Appendix B
FY 2010 Notices of IT Findings and Recommendations at FLETC

Notice of Findings and Recommendations (NFR) – Definition of Severity Ratings:

Each NFR listed in Appendix B is assigned a severity rating from 1 to 3 indicating the influence on the DHS Consolidated Independent Auditors' Report.

1 – Not substantial

2 – Less significant

3 – More significant

The severity ratings indicate the degree to which the deficiency influenced the determination of severity for consolidated reporting purposes.

These ratings are provided only to assist the DHS in prioritizing the development of its corrective action plans for remediation of the deficiency.

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2010

Notice of Findings and Recommendations – Detail

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
FLETC-IT-10-01	During our FY 2010 review of FLETC's configuration management policies and procedures, we noted that FLETC does not conduct the following: • Momentum and GAN changes are not being documented throughout the change control process from the testing of changes to the final approval of the changes prior to implementation, and; • Distribution and implementation of Momentum and GAN changes are not being controlled.	The FLETC management will update and enforce current procedures to ensure changes are fully documented throughout the change control process to include the results of testing the change, review of the change test results, and final approval to proceed with the implementation.	X		2
FLETC-IT-10-02	During the FY 2009 financial statement audit, we noted several weaknesses with the logical access controls for the GAN. During our review in FY2010, we reviewed the logical access controls over the GAN. Per our review, we noted that FLETC has remediated all of the logical access controls over the GAN; however, KPMG noted that the GAN was configured to reset the lockout counter after 20 minutes. This does not meet the DHS 4300A requirement of 24 hours. Upon notification, FLETC immediately remediated the configuration issue. However, the configuration was inappropriately configured for the majority of the fiscal year.	Due to remediation of this finding within the fiscal year, no recommendation is required.		X	3
FLETC-IT-10-03	In FY 2009, KPMG conducted After-Hours walkthrough testing to complement our IT audit testing efforts as part of the FY 2010 DHS Financial Statement Audit and Audit of Internal Control over Financial Reporting. We also performed after-hours	Finance Division, Building 66 Safeguarding of PII and Credit Card data: Modifications to Building 66 have recently been completed which provide secure file storage rooms and entry controls for all access points in the building. A Standard		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	physical security testing to identify risks related to non-technical aspects of IT security. These non-technical IT security aspects include physical access to equipment that houses financial data and information residing on the desks of FLETC personnel, which could be used by others to inappropriately access financial information. For our review in FY 2010 follow up test work was performed at various FLETC buildings in the Glynco, Georgia complex. The designated FLETC Technical Point of Contact and representatives from the DHS Office of Inspector General, the DHS Office of Information Security, and the FLETC Office of Physical Security accompanied KPMG to monitor testing and validate the results. After gaining access to the facilities, we inspected a random selection of desks and offices, looking for items such as improper protection of system passwords, unsecured information system hardware, documentation marked FOUO, and unlocked network sessions. Our selection of desks and offices was not statistically derived, and therefore we are unable to project results to the component or department as a whole. We reviewed over 90 desks and cubicles within the four locations.	Operating Procedure (SOP) will be drafted to address Safeguarding of PII and Credit Card data in the Finance Division, implement use of the secure file storage rooms, and address entry controls for access points in the building. This will be developed and implemented by November 15, 2010. Additionally, specific requirements for Safeguarding of PII and Credit Card data will be added to each Finance Division employee's FY2011 (and future) Annual Performance Work Plan to ensure there is no misunderstanding regarding each employee's responsibilities in this area. Finance Office, Building 66 User Name and Passwords: Remedial training will be conducted regarding safeguarding User Name and Passwords. Additionally, specific requirements for safeguarding User Name and Passwords will be added to each Finance Division employee's FY2011 (and future) Annual Performance Work Plan to ensure there is no misunderstanding regarding each employee's responsibilities in this area. For the CIO Operations and Support Division (OSD) in Bldg 681, remedial training will be conducted to ensure employees and contractors lock their doors and safeguard sensitive information. OSD will ensure the workstation screensaver feature is enabled on its workstations.			
FLETC-IT-10-04	During the FY 2009 financial statement audit, KPMG determined that logs of auditable events in the GAN are not being reviewed to identify potential incidents.	FLETC's current SIM solution provides no capability to correlate or aggregate audit logs which results in an arduous, un-trackable and		X	2

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	During our FY 2010 review, KPMG determined that FLETC has implemented the Security Information Management System (SIM) with capabilities to manage and store logs of auditable events. However, we determined that management does not have a formal process for reviewing the audit logs on a periodic basis.	unmanageable audit log review process when handling millions of records each day. FLETC is currently in the process of procuring ArcSight ESM as a replacement SIM solution to address these and other shortcomings with the current solution. ArcSight ESM allows for both simplified and exceptionally complex event correlation rule authorship. FLETC will deploy the ArcSight ESM solution during FY 2011. Users, such as ISSOs, will be provided focused dashboards with correlated information pertinent to their areas of responsibility. Audit logs will be reviewed as correlated and aggregated data and can be drilled down to in detail and reviewed when suspicious or anomalous records are found. Customized reports and automated alerts will be configured for each system and tailored for the audit log reviewer. Audit logs of access to the SIM itself will also be generated and reviewed to ensure users such as ISSO's and the SOC are utilizing the system and reviewing audit records and responding to the configured automated alerts in a timely manner.			
FLETC-IT-10-05	During the FY 2009 financial statement audit, KPMG determined that access control weaknesses existed over Momentum access authorizations for user's profiles created or modified during the fiscal year. During the FY 2010 financial statement audit, KPMG determined that access control weaknesses still existed over Momentum access authorizations for user's profiles created or modified during the fiscal year. Specifically, we learned that new users and profile	FLETC has implemented profile logging, however, due to the overwhelming volume of events logged by the system, this has proven to be unusable in terms of identifying relevant activity. FLETC is working to better analyze and manage the profile logging reports. An SOP will be drafted to implement management oversight for Momentum access authorizations for user's profiles created or modified during the fiscal year. This process will be developed and implemented		X	3

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	changes are not being tracked by FLETC.	by November 30, 2010.			
FLETC-IT-10-06	During the FY 2009 financial statement audit, we noted several weaknesses around access controls for SIS including: • SIS is configured to have a password history of two passwords stored • SIS is not configured to reset the account failed logon counter • Users were not locked out after three invalid access attempts. • SIS system administrators share a 'root' username and password to perform administrative responsibilities. • A sample of audit logs that track changes to system data could not be provided. • User profile creation is not tracked and a listing of profile creation dates could not be provided. • Evidence of periodic review of user accounts could not be provided. In FY 2010, we inquired with FLETC and noted that although some corrective actions have taken place, the following has not yet been implemented. • Users are not being locked out after three invalid attempts. • SIS password length minimum is configured a minimum of six. • SIS does not require a combination of alphabetic, numeric, and special characters. • Audit logs that track changes to system data are not being reviewed.	FLETC will update the existing Risk Acceptance to include the password exceptions noted in the condition.		X	2

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2010

NFR #No	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
	• Profile creation and changes are not being tracked and a listing of profile updates could not be provided. • Periodic review of user accounts is not being conducted.				

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2010

Appendix C

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

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2010

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
FLETC-IT-09-03	Momentum System Software is Not Logged or Reviewed.	X	
FLETC-IT-09-26	System Engineering Lifecycle is not finalized.	X	
FLETC-IT-09-31	Configuration Management Weaknesses on the Procurement Desktop, Momentum, and GSS.	X	
FLETC-IT-09-33	Momentum Audit Logs are not Reviewed.		10-04
FLETC-IT-09-34	GAN audit logs are not reviewed.		10-05
FLECT-IT-09-35	Weak access controls around Momentum.		10-02
FLETC-IT-09-36	Ineffective logical access controls over the GAN.		10-03
FLETC-IT-09-37	Physical Security and Security Awareness Issues Identified during Enhanced Security Testing.		10-06
FLETC-IT-09-38	Ineffective logical access controls over SIS.	X	

Federal Law Enforcement Training Center
U. S. Department of Homeland Security
1131 Chapel Crossing Road
Glynco, Georgia 31524

Homeland Security

February 23, 2011

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General
Information Technology Audits

FROM: Sandy H. Peavy
Assistant Director/Chief Information Officer
Chief Information Officer Directorate

SUBJECT: Response to Draft Audit Report - *Information Technology Management Letter for the Federal Law Enforcement Training Center Component of the FY2010 DHS Financial Statement Audit – For Official Use Only OIG Project No. 11-029-ITA-FLETC*

The Federal Law Enforcement Training Center (FLETC) appreciates your efforts in assessing the effectiveness of our general Information Technology (IT) controls supporting the FLETC's financial processing environment and related IT infrastructure. The FLETC welcomes your observations and recommendations for ensuring a secure and compliant operational environment.

We have completed our review of the draft management letter from the independent accounting firm of KPMG LLP (KPMG) titled *Information Technology Management Letter for the Federal Law Enforcement Training Center Component of the FY 2010 DHS Financial Statement Audit-For Official Use Only* and concur with the Notice of Findings and Recommendations (NFRs). The FLETC continues to make progress by remediating many of its prior years' IT control weaknesses.

The FLETC is committed to improving and enhancing the security and integrity of its financial reporting process and overall IT security posture.

Point of contact for additional information or questions is the FLETC Chief Information Security Officer, Jeffery W. Johnson, (912) 267-2136.

cc: Director
Deputy Director
Chief Financial Officer

www.fletc.gov

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Chief of Staff
Deputy Chief of Staff
Executive Secretariat
Under Secretary, Management
Director, FLETC
DHS Chief Information Officer
DHS Chief Financial Officer
Chief Financial Officer, FLETC
Chief Information Officer, FLETC
Chief Information Security Officer
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
DHS GAO OIG Audit Liaison
Chief Information Officer, Audit Liaison
Audit Liaison, FLETC

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

• Call our Hotline at 1-800-323-8603;

• Fax the complaint directly to us at (202) 254-4292;

• Email us at DHSOIGHOTLINE@dhs.gov; or

• Write to us at:
DHS Office of Inspector General/MAIL STOP 2600,
Attention: Office of Investigations - Hotline,
245 Murray Drive, SW, Building 410,
Washington, DC 20528.

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