



Department of Homeland Security Office of Inspector General

Information Technology Management Letter for the FY 2009 Federal Law Enforcement Training Center Financial Statement Audit





Homeland
Security

April 30, 2010

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 Federal Law Enforcement Training Center financial statement audit as of September 30, 2009. It contains observations and recommendations related to information technology internal control that were summarized within the *Independent Auditors' Report*, dated December 31, 2009 and represents the separate limited distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit procedures at FLETC in support of the FLETC FY 2009 consolidated financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated December 31, 2009, and the conclusions expressed in it. We do not express opinions on FLETC's consolidated financial statements or internal control or conclusions 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.

A handwritten signature in black ink, appearing to read "Frank Deffer".

Frank Deffer
Assistant Inspector General
Information Technology Audits



KPMG LLP
2001 M Street, NW
Washington, DC 20036

December 31, 2009

Inspector General
U.S. Department of Homeland Security

Chief Information Officer
Federal Law Enforcement Training Center

Chief Financial Officer
Federal Law Enforcement Training Center

Ladies and Gentlemen:

We have audited the consolidated balance sheets of the Federal Law Enforcement Training Center (FLETC), a component of the U.S. Department of Homeland Security (DHS), as of September 30, 2009 and 2008, and the related consolidated statements of net cost, changes in net position, and the combined statement of budgetary resources (hereinafter referred to as “consolidated financial statements”) for the years then ended. In planning and performing our audit of the consolidated financial statements of FLETC, in accordance with auditing standards generally accepted in the United States of America, we considered FLETC’s internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the consolidated financial statements but not for the purpose of expressing an opinion on the effectiveness of FLETC’s internal control. Accordingly, we do not express an opinion on the effectiveness of FLETC’s internal control.

In planning and performing our fiscal year 2009 audit, we considered FLETC’s internal control over financial reporting by obtaining an understanding of the design effectiveness of FLETC’s internal control, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls as a basis for designing our auditing procedures for the purpose of expressing our opinion on the consolidated financial statements. To achieve this purpose, we did not test all internal controls relevant to operating objectives as broadly defined by the *Federal Managers’ Financial Integrity Act of 1982*. The objective of our audit was not to express an opinion on the effectiveness of FLETC’s internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of FLETC’s internal control over financial reporting.

A deficiency in internal control 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.

Our audit of FLETC as of, and for the year ended, September 30, 2009 disclosed a material weakness in the areas of information technology (IT) access controls, configuration management, and security management. These matters are described in the *IT General Control Findings by Audit Area* section of this letter.

The material weakness described above is presented in our *Independent Auditors’ Report*, dated December 31, 2009. This letter represents the separate limited distribution report mentioned in that report.



The control deficiencies described herein have been discussed with the appropriate members of management, and communicated through Notice of Finding and Recommendations (NFRs). Our audit procedures are designed primarily to enable us to form an opinion on the consolidated financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. 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.

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 the FY 2009 FLETC consolidated financial statement audit 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 certain additional matters have been presented in a separate letter to the Office of Inspector General and the FLETC Director dated December 31, 2009.

This communication is intended solely for the information and use of DHS and FLETC management, DHS Office of Inspector General, the 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, 2009

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

	Page
Objective, Scope, and Approach	2
Summary of Findings and Recommendations	3
IT General Control Findings by Audit Area	4
Findings Contributing to a Material Weakness in IT	4
Access Controls and Configuration Management	4
Security Management, Including After-Hours Physical Security Testing	5
Application Control Findings	9

APPENDICES

Appendix	Subject	Page
A	Description of Key FLETC Financial Systems and IT Infrastructure within the Scope of the FY 2009 FLETC Consolidated Financial Statement Audit Engagement	10
B	FY 2009 Notices of IT Findings and Recommendations at FLETC	12
	- Notice of Findings and Recommendations – Definition of Severity Ratings	13
C	Status of Prior Year Notices of Findings and Recommendations and Comparison to Current Year Notices of Findings and Recommendations at FLETC	19
D	Management’s Comments and OIG Response	22
E	Report Distribution	23

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2009

OBJECTIVE, SCOPE, AND APPROACH

We were engaged to perform an audit of the Federal Law Enforcement Training Center's (FLETC) consolidated balance sheets of September 30, 2009 and 2008. In connection with our audit of FLETC's consolidated financial statements we performed an evaluation of information technology general controls (ITGC) to assist in planning and performing our audit. The *Federal Information System Controls Audit Manual (FISCAM)*, issued by the Government Accountability Office (GAO), formed the basis of our ITGC evaluation procedures. The scope of the ITGC evaluation is described further in Appendix A.

The 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 consolidated financial statement audit. The 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. The FISCAM defines the following five control functions to be essential for 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 and 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 the implementation of unauthorized changes to information system resources (software programs and hardware configurations) and that provide 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, 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 selected FLETC facilities, and focused on test, development, and production devices that directly support key general support systems.

- *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.

We also 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.

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2009

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During FY 2009, FLETC took corrective action to address many of its prior year IT control weaknesses. The upgrade of the Financial Accounting and Budgeting System (FABS, also called Momentum) and the installation of new hardware near the end of FY 2008 improved the overall security structure at FLETC. However, during FY 2009, we continued to identify IT general control weaknesses that impacted FLETC's financial data. The most significant control deficiencies from a consolidated financial statement audit perspective related to controls over access and configuration management and the weaknesses over physical security and security awareness. Collectively, these 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. In addition, these control deficiencies negatively impacted FLETC's internal controls over financial reporting and its operation. We consider these deficiencies to collectively represent a material weakness under standards established by the American Institute of Certified Public Accountants (AICPA). Based upon the results of our test work, we noted that FLETC also did not fully comply with the requirements of the *Federal Financial Management Improvement Act* (FFMIA).

Of the 10 findings identified during our FY 2009 testing, 6 were new IT findings. These findings represent control deficiencies in three of the five FISCAM key control areas. The control areas are specifically, 1) lack of management and review of system audit logs, 2) ineffective account management issues involving user profiles, new user access, active terminated user accounts, generic user accounts, and lack of account recertifications, 3) inadequate configuration management, and 4) 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 FLETC's 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 upon their system capabilities and available resources.

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2009

IT GENERAL CONTROL FINDINGS BY AUDIT AREA

Findings Contributing to a Material Weakness in IT

Conditions: During FY 2009, we noted the following IT general control and financial system functionality deficiencies that in the aggregate are considered a material weakness.

1. Access Controls and Configuration Management:

- Access and configuration management weaknesses on the Glynco Administrative Network (GAN) and the servers that support Momentum and the Student Information System (SIS). These weaknesses included default configuration settings, role and group policies, and weak password management. *Note: Detailed vulnerability assessment results were previously provided to FLETC and included the risk level.*
- System Engineering Life Cycle (SELV) for Momentum is not finalized.
- Momentum system software event audit logs are not being captured and reviewed.
- Password configuration settings for Linux, which support Momentum system software, allow 6 failed logon attempts before the account is locked.
- Momentum and the 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 GAN were noted as follows:
 - The GAN prohibits password reuse for 6 generations, which does not meet the DHS 4300A requirement of 8 password generations.
 - The GAN resets the account failed logon counter after 60 minutes, which does not meet the DHS 4300A requirement of 24 hours.
 - Generic user IDs, i.e. 'vcusersqp', 'vcusersqlar', 'PACSUser', 'BESAdmin', and other generic account descriptors were identified. In addition, several users have access to these accounts.
 - New user access authorization forms are not maintained.
 - Fourteen instances of active user accounts for terminated employees were identified.
 - A periodic review over GAN users is not performed.
- Weak logical access controls over the SIS were noted as follows:
 - A history of 2 passwords is stored; this does not meet the DHS 4300A requirement of 8 remembered passwords.
 - SIS is configured to have a minimum password age of 5 days; this does not meet DHS 4300A requirements of 7 days.
 - 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).
 - System administrators share the 'root' username and password to perform administrative responsibilities.

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2009

- A sample of audit logs that track changes to system data could not be provided.
- Invalid user access attempts were not tracked and monitored until March 2009. Since this weakness was corrected during the fiscal year, no recommendation will be stated.
- 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.

2. Security Management including After-Hours Physical Security Testing:

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
	OIT Office, Building 681	Finance Office, Building 66	BFD, Procurement, and SIS, Building 93	Telecommunications Facility, Building 94	
User Name and Passwords	1	9	21	53	84
For Official Use Only (FOUO)	2	1	0	1	4
Keys/Badges	0	0	0	7	7
Personally Identifiable Information (PII)	0	80	2	1	83
Server Names/IP Addresses	0	0	0	0	0
Laptops	3	0	2	1	6
External Drives	0	0	0	2	2
Credit Cards	0	12	0	0	12
Classified Documents	0	0	0	0	0
Other - Describe	2 users still logged into DHS systems without a screensaver	1 user still logged into DHS systems without a screensaver	0	1 user still logged into DHS systems without a screensaver	4
Total Exceptions by Location	8	103	25	66	202

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2009

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 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:

Access Controls and Configuration Management:

1. Redistribute procedures and train employees on continuously monitoring and mitigating vulnerabilities. In addition, we recommend that FLETC periodically monitor the existence of unnecessary services and protocols running on their servers and network devices, in addition to deploying patches.
2. Perform vulnerability assessments and penetration tests on all office IT systems within FLETC, from a centrally managed location with a standardized reporting mechanism that allows for trending on a regularly scheduled basis in accordance with National Institute of Standards and Technology (NIST) guidance.
3. Develop a more thorough approach to track and mitigate configuration management vulnerabilities identified during monthly scans. FLETC should monitor the vulnerability reports for necessary or required configuration changes to their environment.
4. Develop a process to verify that systems identified with "HIGH/MEDIUM Risk" configuration vulnerabilities do not appear on subsequent monthly vulnerability scan reports, unless they are verified and documented as a false-positive. All risks identified during the monthly scans should be mitigated immediately and not be allowed to remain dormant.
5. Enable audit logging over all Momentum system software and ensure that logs are maintained and proactively reviewed by FLETC IT management.
6. Enforce existing FLETC policy and procedures over maintenance and review of Momentum security violation logs.
7. Establish and implement procedures to document and review logs of auditable events on the GAN.
8. Activate logs for monitoring Momentum user profile creation and modifications.
9. Implement the corrective actions identified during the audit vulnerability assessment as identified in the issued NFR of the audit.
10. Perform periodic scans of the FLETC network environment, including the financial processing environment, for the identification of vulnerabilities, in accordance with NIST SP 800-42, and implement corrective actions to mitigate the risks associated with any vulnerabilities identified during periodic scans.
11. Establish a process to ensure that GAN and Linux (Momentum system software) are configured to meet minimum DHS password configuration requirements.

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2009

12. Remove all GAN and SIS generic/shared accounts and conduct periodic reviews of user access lists to ensure compliance.
13. Establish and enforce procedures for the completion and maintenance of user access forms for GAN and SIS.
14. Enforce procedures for the removal of transferred, and, or terminated users within the GAN upon their separation from FLETC.
15. Establish and implement policies and procedures for recertification of GAN user privileges. This process should include a method to document user recertification and a process to maintain evidence of reviews.
16. Establish a process to ensure the SIS is configured to meet minimum DHS password and system configuration requirements.
17. Retain audit trail records in accordance with DHS policies in order to support potential incidents within the system, and for review of user privileges.
18. FLETC has effectively implemented the DHS SELC as of April 2009. Therefore, no recommendation will be stated.

Security Management:

1. Ensure that users are trained and aware of safeguarding login credentials, locking network sessions to DHS systems, and locking any sensitive information, media containing sensitive information, or data not suitable for public dissemination in secure locations when not in use.
2. Effectively limit access to DHS buildings, rooms, work areas, spaces, and structures housing IT systems, equipment, and data to authorized personnel.

Cause and Effect

FLETC is not continuously monitoring their vulnerability assessment scans for configuration management vulnerabilities. As a result, default system and application configuration installations on the FLETC's Glynco Administrative Network (GAN), Financial Accounting and Budgeting System (FABS), and Student Information System (SIS) increase the possibility of compromise the availability, integrity, and confidentiality of financial data on the network. This could jeopardize the information system controls environment to security breaches, unauthorized access, service interruptions, and denial of service attacks.

FLETC has been relying on the full implementation of the Security Information Management (SIM) system, which will monitor Momentum system software and the GAN audit logs. However, this has not occurred to date due to lack of staffing. In addition, due to the lack of management oversight, the Momentum approval and security logs review procedures are not being adhered to. The lack of

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2009

audit logs may cause security related incidents to go unnoticed and uninvestigated, thus allowing potential unauthorized system software changes to deploy into the production environment.

FLETC management has not enabled the Momentum audit logging system setting, which would capture user profile creation and modification. Without logging of new users and profile changes, FLETC would be unaware of any unauthorized additions or changes to profiles within Momentum. This could also lead to a violation of both separation of duties and least privilege principles in practice.

Due to the lack of management oversight, GAN logical access controls and Momentum system software access controls have not been strengthened to meet DHS IT security compliance. In addition, FLETC management considers the SIS to have a low impact on operations; therefore, sufficient controls have not been implemented. Having weak system access controls increases the risk of unauthorized individuals gaining access to and improperly modifying or destroying data. Also, having generic/shared user accounts on a production system reduces the audit and accountability of users within the system. Without documenting and approving access forms to applications, management is unaware of the system access an individual may possess. This could lead to a violation of both separation of duties and least privilege principles. Additionally, unauthorized users may obtain access to the systems. Without access review and recertification procedures being formally documented, reviewers do not have an IT standard for effectively conducting the recertification of GAN accounts. This could lead to the risk of potentially allowing users to have account privileges that are needed no longer, or, initially should not have been granted.

FLETC management has not ensured that personnel are adequately trained and aware of the basic IT security requirements and policies described by DHS and FLETC to protect their login credentials, lock network sessions to DHS systems, secure information system hardware, and securely store/limit access to FOUO and PII data. The failure to control access to sensitive IT resources and FLETC documentation potentially could result in the theft or destruction of FLETC assets, unauthorized access to sensitive information, and disruptions in processing of FLETC financial systems. Additionally, FLETC personnel who are not trained adequately to protect their login credentials present an increased risk of unauthorized access to sensitive information from external and internal threats.

Criteria: The *Federal Information Security Management Act (FISMA)* passed as part of the *Electronic Government Act of 2002*, mandates that Federal entities maintain IT security programs in accordance with OMB and NIST guidance. OMB Circular No. A-130, *Management of Federal Information Resources*, and various NIST guidelines describe specific essential criteria for maintaining effective general IT controls. FFMIA sets forth legislation prescribing policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems. The purpose of FFMIA is: (1) to provide for consistency of accounting by an agency from one fiscal year to the next, and uniform accounting standards throughout the Federal Government; (2) require Federal financial management systems to support full disclosure of Federal financial data, including the full costs of Federal programs and activities; (3) increase the accountability and credibility of federal financial management; (4) improve performance, productivity and efficiency of Federal Government financial management;

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2009

and, (5) establish financial management systems to support controlling the cost of Federal Government. We also assessed FLETC's compliance with DHS Sensitive System Policy Directive 4300A.

APPLICATION CONTROL FINDINGS

We did not identify any findings in the area of application controls during the fiscal year 2009 FLETC consolidated financial statement audit engagement.

MANAGEMENT COMMENTS AND OIG RESPONSE

We obtained written comments on a draft of this report from the FLETC CIO. Generally, the FLETC agreed with all of our findings and recommendations. The FLETC has developed a remediation plan to address these findings and recommendations. We have included a copy of the comments 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, 2009**

Appendix A

**Description of Key FLETC Financial Systems and IT
Infrastructure within the Scope of the FY 2009 FLETC
Consolidated Financial Statement Audit**

**Department of Homeland Security
Federal Law Enforcement Training Center**
Information Technology Management Letter
September 30, 2009

Below is a description of significant FLETC financial management systems and supporting IT infrastructure included in the scope of the FY 2009 FLETC Consolidated Financial Statement Audit.

Location of Audit: FLETC Headquarters in Glynco, Georgia and the FLETC field office in Cheltenham, Maryland.

Key Systems Subject to Audit:

- *Financial Accounting and Budgeting System (FABS) also called Momentum:* FLETC's core financial management system that processes financial documents generated by various FLETC divisions in support of procurement, payroll, budget and accounting activities. All financial, procurement and budgeting transactions where FLETC is involved are processed by Momentum.
- *Student Information System (SIS):* The system captures and facilitates the FLETC student registration process and billing. SIS stores, processes, and transmits Sensitive But Unclassified (SBU) information, which includes individual student personal information. Additional data types include specific course information (e.g., course numbers, dates, associated agencies, locations, and billing costs).

**Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2009**

Appendix B

FY 2009 Notices of IT Findings and Recommendations at FLETC

**Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2009**

Notices of Findings and Recommendations – Definition of Severity Ratings:

Each NFR listed in Appendix B is assigned a severity rating from 1 to 3 indicating the influence on the FLETC Consolidated Financial Statement Audit.

- 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 rating are provided to assist the FLETC in the development of corrective action plans for remediation of the deficiency.

**Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2009**

Notification of Findings and Recommendations – Detail

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
FLETC-IT-09-03	<p>We determined that SOP 4250, which has been in effect for the entire fiscal year, was last updated on May 12, 2009 and that FLETC has developed a manual control for the installation of system software for Momentum. Specifically, logs of file changes to the Momentum UNIX servers are reviewed monthly. Therefore, this condition of the prior weakness has been partially corrected.</p> <p>We also determined that FLETC is still in the process of implementing the Security Information Management System (SIM) to compile audited events of Oracle and other system software for review by FLETC personnel. FLETC management has confirmed that logs of Oracle are not being reviewed to identify potential anomalies or incidents. Due to the lack of audit logging procedures around system software for Momentum, this NFR will be reissued.</p>	<p>We recommend that FLETC enable audit logging over all Momentum system software and ensure that logs are maintained and proactively reviewed by management.</p>		X	3
FLETC-IT-09-04	<p>We determined that FLETC has implemented DHS's System Engineering Lifecycle (formally called SDLC) into their business processes, and that it is promulgated to personnel involved in the change management process. However, we determined that implementation did not occur until April 2009. As a result, we will be reissuing this NFR with no recommendation since the condition has existed for a majority of the fiscal year.</p>	<p>As FLETC has effectively put into place procedures over the implementation of DHS' SELC effective April 2009, no recommendation will be offered.</p>		X	3

**Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter**
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
FLETC-IT-09-26	<p>During the internal vulnerability assessment efforts of FLETC's Glyco Administrative Network (GAN), Financial Accounting and Budgeting System (FABS), and Student Information System (SIS) systems we identified several High/ Medium Risk vulnerabilities, related to Configuration Management and Password Management. We confirmed that security configuration management weaknesses (i.e., default configuration settings, role and group policies, password policy, and user account management) continue to exist on hosts supporting FLETC. The conditions are exploitable as an insider without specific knowledge of the operation of the system or the applications hosted on that system. These conditions can be found in the table within the actual NFR.</p>	<p>Implement the corrective actions for the recommendations listed within the NFR.</p>		X	3
FLETC-IT-09-31	<p>We determined that in January 2009, FLETC implemented a Standard Operating Procedure (SOP) #60 titled, "Monthly Review of Security and Approval Logs", which requires management review and sign off. However, FLETC was unable to provide documentation supporting the management review of approval logs for April, May, June, and July. In addition, FLETC was unable to provide evidence of management review of the security violation logs for June and July 2009.</p>	<p>We recommend that FLETC enforce their policies and procedures for the maintenance and periodic review of audit logs for Momentum.</p>		X	3

**Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter**
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
FLETC-IT-09-33	<p>We determined that logs of auditable events in the LAN are not being reviewed to identify potential anomalies or incidents. FLETC is in the process of implementing SIM with the capabilities to manage logged auditable events for review by personnel. We determined that while the SIM is being implemented, FLETC does not have an alternative procedure for the review of these logs.</p>	<p>We recommend that FLETC establish and implement procedures to document and review logs of auditable events in the LAN.</p>	X		3
FLETC-IT-09-34	<p>We determined that access control weaknesses existed over the Momentum access authorizations for user profiles created or modified during the fiscal year. Specifically, we learned that profile creation and modification is not tracked and a listing of events could not be provided.</p> <p>We noted several weaknesses with logical access controls related to GAN:</p> <ul style="list-style-type: none"> • The GAN is configured to prohibit password reuse for 6 generations, which does not meet the DHS standard of 8 password generations. • The GAN is configured to reset the account failed logon counter after 60 minutes, which does not meet the DHS standard of 24 hours. • Several user IDs were identified as having excessive access. • Supporting documentation for new user authorizations to the GAN could only be provided for 10 users out of 25 users sampled. 	<p>We recommend that FLETC activate the logs for tracking the addition of new users and profile changes to Momentum.</p>	X		3
FLETC-IT-09-35	<p>We noted several weaknesses with logical access controls related to GAN:</p> <ul style="list-style-type: none"> • The GAN is configured to prohibit password reuse for 6 generations, which does not meet the DHS standard of 8 password generations. • The GAN is configured to reset the account failed logon counter after 60 minutes, which does not meet the DHS standard of 24 hours. • Several user IDs were identified as having excessive access. • Supporting documentation for new user authorizations to the GAN could only be provided for 10 users out of 25 users sampled. 	<p>We recommend that FLETC Management:</p> <ul style="list-style-type: none"> • Establish a process to ensure the GAN is configured to meet minimum DHS password configuration requirements. • Remove all generic/shared accounts and conduct period reviews of the user access lists to ensure compliance. • Establish and enforce procedures for the completion and maintenance of user access forms for the GAN. • Enforce procedures for the removal of transferred/terminated users within the GAN upon their separation from FLETC. 	X		3

**Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter**
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
FLETC-IT-09-36	<ul style="list-style-type: none"> Fourteen separated employees still had active user accounts to the GAN. Formalized procedures are not in place for periodic reviews over GAN users. <p>During our after hours physical testing, we identified 84 password discrepancies, 4 For Official Use Only Violations, 7 unsecured ID badges/keys, 83 Personally Identifiable Information violations, 6 unsecured laptops, 2 unsecured external drives, 12 unsecured credit cards, and 4 users logged into a system without an active screen saver set.</p>	<ul style="list-style-type: none"> Establish and implement policies and procedures for recertification of GAN user privileges. <p>We recommend that FLETC management implement processes to:</p> <ul style="list-style-type: none"> Ensure that users are trained and aware of safeguarding login credentials, locking network sessions to DHS systems, and locking any sensitive information, media containing sensitive information, or data not suitable for public dissemination in secure locations when not in use. Effectively limit access to DHS buildings, rooms, work areas, spaces, and structures housing IT systems, equipment, and data to authorized personnel. 	X		3
FLETC-IT-09-37	<p>We noted several weaknesses relating to logical access controls for the SIS. Specifically, we determined the following:</p> <ul style="list-style-type: none"> SIS is configured to have a password history of 2 passwords stored that does not meet the DHS 4300A requirement of 8 remembered passwords. SIS is configured to have a minimum password age of 5 days that does not meet DHS 4300A requirements of 7 days. 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. Users were not locked out until after 6 invalid 	<p>We recommend that FLETC management:</p> <ul style="list-style-type: none"> Establish a process to ensure the SIS is configured to meet minimum DHS password configuration requirements. Adjust system configuration settings to lock out users after 3 invalid logon attempts as designated by DHS policies. Remove all generic/shared accounts and conduct periodic reviews of the user access lists to ensure compliance. Retain audit trail records in accordance with DHS policies in order to support potential incidents within the system, and for review of 	X		3

**Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter**
September 30, 2009

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Severity Rating
FLETC-IT-09-38	<p>attempts to access the application.</p> <ul style="list-style-type: none"> • SIS system administrators share the 'root' username and password to perform administrative responsibilities. • A sample of audit logs that track changes to system data could not be provided. • Invalid user access attempts were not tracked and monitored until March 2009. . • 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. <p>We determined that weak access controls exist over Momentum's system software. Specifically, we noted that the password configuration settings for Linux, which supports Momentum, is set to allow a user to attempt to logon 6 times before the account is locked out.</p>	<p>user privileges.</p> <ul style="list-style-type: none"> • Activate tracking for the addition of new users to SIS. • Since this weakness was corrected during the fiscal year, no recommendation will be stated. 	X		3

**Department of Homeland Security
Federal Law Enforcement Training Center**
Information Technology Management Letter
September 30, 2009

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, 2009

		Disposition	
NFR No.	Description	Closed	Repeat
FLETC-IT-08-01	Momentum Configuration Management Needs Improvement	X	
FLETC-IT-08-02	Procurement Desktop Configuration Management Needs Improvement	X	
FLETC-IT-08-03	Installation of Momentum System Software is not Logged or Reviewed		09-03
FLETC-IT-08-04	The SDLC for Momentum is not Finalized		09-04
FLETC-IT-08-05	Momentum Backups are not Tested	X	
FLETC-IT-08-06	The Momentum Contingency Plan is not Completed	X	
FLETC-IT-08-07	Incidents are not Tracked in an Incident Response Management System	X	
FLETC-IT-08-08	Lack of Policies and Procedures over Incompatible Duties within Procurement Desktop	X	
FLETC-IT-08-09	Telecom Room Access Controls Need Improvement	X	
FLETC-IT-08-10	Momentum and Procurement Desktop Access Controls Need Improvement	X	
FLETC-IT-08-11	IT Security Awareness Training is in Draft Form	X	
FLETC-IT-08-12	Policies and Procedures over Mobile Code Technologies are not Developed	X	
FLETC-IT-08-13	Policies and Procedures for Review of Momentum Audit Logs are not Developed	X	
FLETC-IT-08-14	Policies and Procedures for Restricting Access to Momentum System Software are not Developed	X	
FLETC-IT-08-15	Policies and Procedures for Segregating Incompatible Duties in Momentum are not Developed	X	
FLETC-IT-08-16	Policies and Procedures over VoIP Technologies are not Developed	X	
FLETC-IT-08-17	Background Investigations for Contractors are not Consistently Performed	X	
FLETC-IT-08-18	Procurement Desktop Audit Logs Need Improvement	X	
FLETC-IT-08-20	Access to FLETC LAN is not Effectively Controlled	X	
FLETC-IT-08-21	FLETC Manual 4300: IT System Security Program and Policy are not Finalized	X	
FLETC-IT-08-22	Access Controls over Procurement Desktop are not Effective	X	
FLETC-IT-08-23	Lack of Procedures for Recertifying Procurement Desktop Users	X	

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2009

		Disposition	
NFR No.	Description	Closed	Repeat
FLETC-IT-08-24	Momentum/Procurement Desktop Contingency Plan is not Maintained at the Alternate Processing Site	X	
FLETC-IT-08-25	Policies and Procedures over Anti-Virus Software for Servers and System Maintenance are not Finalized	X	
FLETC-IT-08-26	Configuration Management Weaknesses on the Procurement Desktop, Momentum, and GSS		09-26
FLETC-IT-08-27	Patch Management Weaknesses on Procurement Desktop and GSS	X	
FLETC-IT-08-29	Procurement Desktop Backups are not Tested	X	
FLETC-IT-08-30	Momentum Users are Granted Inappropriate Super User Access	X	
FLETC-IT-08-31	Momentum Security Violation Events are not Reviewed		09-31
FLETC-IT-08-32	Momentum Segregation of Duties Controls are not Effective	X	

**Department of Homeland Security
Federal Law Enforcement Training Center**
Information Technology Management Letter
September 30, 2009


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



**Homeland
Security**

March 29, 2010

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 FY2009 Federal Law Enforcement
Training Center (FLETC) Financial Statement Audit*

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

We have completed our review of the draft *Office of Inspector General, Information Technology Management Letter for the FY2009 Federal Law Enforcement Training Center Financial Statement Audit* and concur with the Notice of Findings and Recommendations (NFRs). The FLETC has made progress by addressing many of its prior year's IT control weaknesses. However, it is understood that additional corrective action is needed to address the remaining findings and the six new IT recommendations which collectively represent a material weakness.

The FLETC continues to improve and enhance its financial and overall IT security controls in an effort to resolve deficiencies identified in the report.

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

cc: Alan Titus, FLETC Chief Financial Officer

www.fletc.gov

**Department of Homeland Security
Federal Law Enforcement Training Center**
Information Technology Management Letter
September 30, 2009

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
DHS Chief Information Security Officer
Assistant Secretary, Policy
Assistant Secretary for Public Affairs
Assistant Secretary for 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.