



Department of Homeland Security Office of Inspector General

Information Technology Management Letter for the FY 2008 Federal Law Enforcement Training Center Financial Statement Audit (Redacted)



Notice: The Department of Homeland Security, Office of Inspector General has redacted the report for public release. A review under the Freedom of Information Act will be conducted upon request.



**Homeland
Security**

April 27, 2009

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 2008 Federal Law Enforcement Training Center (FLETC) consolidated balance sheet audit as of September 30, 2008. It contains observations and recommendations related to information technology internal control that were not required to be reported in the financial statement audit report (OIG-09-09, November 2008) and represents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit of FLETC's FY 2008 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated December 5, 2008, and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control or make 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 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 cursive script that reads "Richard L. Skinner".

Richard L. Skinner
Inspector General



KPMG LLP
2001 M Street, NW
Washington, DC 20036

March 26, 2009

Inspector General
U.S. Department of Homeland Security

Chief Information Officer
U.S. Federal Law Enforcement Training Center

Chief Financial Officer
U.S. Federal Law Enforcement Training Center

Ladies and Gentlemen:

We have audited the accompanying consolidated balance sheets of the U.S. Department of Homeland Security's (DHS) Federal Law Enforcement Training Center (FLETC) as of September 30, 2008 and 2007, and the related consolidated statements of net cost, and changes in net position, and combined statements of budgetary resources (hereinafter referred to as "consolidated financial statements") for the years then ended. The objective of our audit was to express an opinion on the fair presentation of these consolidated financial statements.

In connection with our fiscal year 2008 audit, we also considered FLETC's internal controls over financial reporting by obtaining an understanding of the FLETC's internal control, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls in order to determine our procedures. We limited our internal control testing to those controls necessary to achieve the objectives described in *Government Auditing Standards* and Office of Management and Budget (OMB) Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements*. We did not test all internal controls relevant to operating objectives as broadly defined by the *Federal Managers' Financial Integrity Act of 1982* (FMFIA).

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 misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects FLETC's ability to initiate, authorize, record, process, or report financial data reliably in accordance with U.S. generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of FLETC's financial statements that is more than inconsequential will not be prevented or detected by FLETC's internal control over financial reporting. A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control.

We identified certain weaknesses during our audit engagement which we would like to bring to your attention. These matters are also described in the *IT General Control Findings by Audit Area* section of this letter.

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



The Table of Contents on the next page identifies each section of the letter. In addition, we have provided: a description of key FLETC financial systems and information technology infrastructure within the scope of the FY 2008 FLETC 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 financial management and reporting internal controls have been presented in a separate letter to the Office of Inspector General and the DHS Chief Financial Officer dated March 26, 2009.

This report is intended solely for the information and use of FLETC management, DHS Office of Inspector General, 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, 2008

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

| | Page |
|--|-------------|
| Objective, Scope and Approach | 1 |
| Summary of Findings and Recommendations | 3 |
| IT General Control Findings by Audit Area | 4 |
| Findings Contributing to a Significant Deficiency in IT | 4 |
| Entity-wide Security Planning | 4 |
| Access Controls | 4 |
| Application Software Development and Change Controls | 4 |
| Service Continuity | 5 |
| System Software | 5 |
| Segregation of Duties | 5 |
| Application Control Finding | 8 |
| Management Comments and OIG Response | 8 |

APPENDICES

| Appendix | Subject | Page |
|-----------------|---|-------------|
| A | Description of Key FLETC Financial Systems and IT Infrastructure within the Scope of the FY 2008 FLETC Financial Statement Audit | 9 |
| B | FY 2008 Notices of IT Findings and Recommendations at FLETC | 11 |
| C | Status of Prior Year Notices of Findings and Recommendations and Comparison to Current Year Notices of Findings and Recommendations | 25 |
| D | Management Comments | 31 |

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008

OBJECTIVE, SCOPE AND APPROACH

We were engaged to perform an audit of the Federal Law Enforcement Training Center's (FLETC) Information Technology (IT) general controls in support of the fiscal year (FY) 2008 FLETC financial statement audit. The overall objective of our engagement was to evaluate the effectiveness of IT general controls of FLETC's financial processing environment and related IT infrastructure as necessary to support the engagement. The *Federal Information System Controls Audit Manual* (FISCAM), issued by the Government Accountability Office (GAO), formed the basis of our audit. The scope of the FLETC IT general controls assessment is 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 six control functions to be essential to the effective operation of the general IT controls environment.

- *Entity-wide security program planning and management (EWS)* – 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 monitor access to computer resources (data, programs, equipment, and facilities) to protect against unauthorized modification, loss, and disclosure.
- *Application software development and change control (ASDCC)* – Controls that help to prevent the implementation of unauthorized programs or modifications to existing programs.
- *System software (SS)* – Controls that limit and monitor access to powerful programs that operate computer hardware and secure applications supported by the system.
- *Segregation of duties (SD)* – Controls that constitute policies, procedures, and an organizational structure to prevent one individual from controlling key aspects of computer-related operations, thus deterring unauthorized actions or access to assets or records.
- *Service continuity (SC)* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

In the current year, FLETC performed a significant upgrade to its [REDACTED] financial reporting software system, from version 3.7 to version 6.1. This upgrade occurred during the period of August 1, 2008 – August 17, 2008 and was conducted by a third party, CACI, Inc. ("CACI"). As such, the automated controls component of FLETC's entity level controls was significantly changed during the period under audit. In addition, there were several control weaknesses identified in the prior year that were not mitigated due to reliance on the impending [REDACTED] application upgrade and the installation of new hardware that would improve the overall IT general controls (ITGC) security structure at FLETC. We designed our scope to perform a pre-conversion ITGC. After the [REDACTED] conversion, we returned to FLETC to perform minimal ITGC test work over the new control environment.

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008

In addition to testing FLETC's general control environment, we performed pre-conversion and post-conversion 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.

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008

SUMMARY OF FINDINGS AND RECOMMENDATIONS

Our audit procedures over IT general controls for FLETC included a review of its procedures, policies, and practices. The IT portion of our audit disclosed matters involving the internal controls over financial reporting and its operation that we consider to be a significant deficiency under standards established by the American Institute of Certified Public Accountants (AICPA). We have noted deficiencies in the design and operation of FLETC's internal controls which could adversely affect the agency's financial statements. We noted deficiencies over entity-wide security planning, access controls, application development and change control, system software, segregation of duties, and service continuity that have contributed to the significant deficiency. The cumulative affect of the deficiencies identified should not lead to material misstatements in the agency-wide financial statements. According to the AICPA, a significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles (GAAP) such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected.

During FY 2008, we noted that FLETC made minimal progress on its control weaknesses. Therefore, many of the prior year Notices of Findings and Recommendations (NFR) could not be closed completely due to the reliance on the impending [REDACTED] application upgrade, the decommissioning of [REDACTED] and the installation of new hardware that would improve the overall ITGC security structure at FLETC. As a result, there was one (1) prior year NFR closed, twenty (27) reissued NFRs, and three (3) new NFRs issued to FLETC.

FLETC management should ensure that there is emphasis placed on the completion, monitoring and enforcement of IT security-related policies and procedures. On-going measures to improve the IT security considerations for key financial systems operated by FLETC and implement effective access controls, segregation of duties and change controls need to be completed.

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.

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008

IT GENERAL CONTROL FINDINGS BY AUDIT AREA

Findings Contributing to a Significant Deficiency in IT

During FY 2008, we noted the following IT and financial system control deficiencies that in aggregate are considered a significant deficiency:

1 Entity-wide Security Planning – we noted:

- Incidents are not tracked from inception to resolution in an incident response management system.
- Background investigations for contractors were not consistently performed.

2 Access controls – we noted:

- The following [redacted] and [redacted] access control weaknesses were identified:
 - Draft policies and procedures exist regarding immediate notification of [redacted] and [redacted] System administrators when users are terminated or transferred.
 - Password configurations for [redacted] [redacted] have been configured to permit passwords to be a minimum of eight characters in length with no complexity requirements, which is not in compliance with DHS 4300A Sensitive Systems Handbook.
- Momentum security violation event audit logs are not reviewed.
- Standard Operating Procedures (SOPs) for the use and installation of [redacted] [redacted] [redacted] ([redacted] technologies have been documented, but are not finalized.
- Security inspections for all [redacted] networks have not been completed.
- Configuration Management weaknesses on [redacted] [redacted] [redacted] and the [redacted] [redacted] were identified. These weaknesses included account management, auditing, database configuration and password management weaknesses.
- Patch Management weaknesses on hosts and database supporting the [redacted] [redacted] applications and [redacted] [redacted] [redacted] were identified. Additionally, the same servers were identified as having excessive access privileges.

3 Application Software Development and Change Controls – we noted:

- Configuration management plans are in draft form for [redacted] and [redacted] [redacted] thus, the plans have not been authorized and fully implemented. Specifically, the following weaknesses were noted:

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008

- Lack of documented test plan standards and procedures;
 - Lack of documented guidance for bug fixes and enhancements, including the emergency change process.
- Excessive access privileges exist, which allows all FLETC domain level users to “modify, read, execute, and write” access to the [redacted] and [redacted] application program libraries.
 - System Development Life Cycle (SDLC) for [redacted] is not finalized.
- 4 Service Continuity – we noted:
- [redacted] server level, [redacted] [redacted] and [redacted] database backups are not periodically tested.
 - The [redacted] contingency plan was tested in May 2008; however, the contingency plan was not updated to reflect the test results.
- 5 System Software – we noted:
- The installation of [redacted] system software has been logged since May 2008; however, the application capturing the data has not been fully implemented, nor are the logs being reviewed by FLETC management.
- 6 Segregation of Duties:
- [redacted] segregation of duties controls for the Accountant role was determined to be ineffective.

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.

- 1 For Entity-wide Security Planning:
- No recommendations will be offered as both conditions were mitigated during the fiscal year.
- 2 For Access Controls:
- Continue with the projected plan for decommissioning the [redacted] [redacted] application.
 - Continue to finalize and implement the “FM 4300: Information Technology System Security Program Policy”, which provides policies for the use of [redacted] technologies.

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008

- Application System Administrators should review security and system-related event logs on a periodic basis.
 - Conduct a security inspection of the [REDACTED] [REDACTED] [REDACTED] installations by completing the FLETC [REDACTED] Security checklist.
 - Implement the corrective actions identified during the audit vulnerability assessment as identified in the issued NFR.
 - Perform periodic scans of the FLETC network environment, including the financial processing environment, for the identification of vulnerabilities, in accordance with National Institute of Standards and Technology (NIST) SP 800-42, and implement corrective actions to mitigate the risks associated with any vulnerabilities identified during periodic scans.
- 3 For Application Software Development Change Controls:
- Ensure that access to the [REDACTED] and [REDACTED] [REDACTED] program libraries are limited to only the Administrators group.
 - Fully implement the Change Control and Configuration Management SOP into the FLETC environment.
 - Continue with the projected plan for decommissioning the [REDACTED] [REDACTED] application.
 - Finalize and implement a SDLC methodology guide for [REDACTED] and ensure that security planning has been incorporated throughout the life cycle.
 - Ensure that the SDLC methodology is promulgated to all personnel involved in the design, development, and implementation process of the SDLC methodology.
- 4 For service continuity:
- Consistently apply the new CIO Backup SOP and periodically test the [REDACTED] server lever and Oracle database backups at least annually in compliance with DHS Information Technology Security Program Publication 4300A.
 - Continue with the projected plan for decommissioning the [REDACTED] [REDACTED] application.
 - Ensure that the results of the [REDACTED] contingency plan test are reflected in the most recent application contingency plan.
- 5 System Software:
- Enable audit logging over the installation of [REDACTED] system and ensure that logs are maintained and proactively reviewed by management.
 - Implement policies and procedures over audit logging of [REDACTED] system software.
- 6 Segregation of Duties:
- Evaluate the access rights for all roles within [REDACTED] and separate the duties for the creation and payment of vouchers.
 - Develop a process to ensure the segregation of duties between the Accountant roles is maintained.

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008

Cause/Effect: The FLETC did not expend the necessary time and resources to correct the [REDACTED] application weaknesses due to the impending upgrade in August 2008. In addition, at the time of the prior year audit, FLETC had plans to replace Procurement Desktop with the DHS Enterprise-wide procurement system [REDACTED] in August 2008; however, that implementation date was moved to October 2008. Therefore, the [REDACTED] weaknesses identified in the prior year were left uncorrected.

Reasonable assurance should be provided that financial system user access levels are limited and monitored for appropriateness. The weaknesses identified within FLETC's access controls increases the risk that employees and contractors may have access to a system that is outside the realm of their job responsibilities. This access could allow a person to intentionally or inadvertently use various functions to alter the integrity of executable files and scripts within the financial system.

The lack of documented configuration management procedures for financial application level bug fixes and enhancements could lead to the risk of inadequate documentation for configuration management changes. Without standardized test plans and procedures, programming flaws with an adverse effect on FLETC's operations could go undetected. Documented procedures will maintain consistency in the implementation of established procedures. Also, the configuration and patch management weaknesses identified in previous audits may increase the risk that the confidentiality, integrity, and availability of system controls and the financial data could be exploited thereby compromising the integrity of financial data used by management and reported in the DHS financial statements.

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.

Federal Financial Management Improvement Act (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; and (5) establish financial management systems to support controlling the cost of Federal Government. In closing, for this year's IT audit we assessed the DHS component's compliance with DHS Sensitive System Policy Directive 4300A.

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008

APPLICATION CONTROL FINDING

During FY 2008, we noted the following application control weakness:

- [REDACTED] users were granted inappropriate superuser access during the post-conversion phase.

Recommendation: No recommendation will be offered as this weakness was remediated during FY 2008 upon notification by KPMG.

MANAGEMENT COMMENTS AND OIG RESPONSE

We obtained written comments on a draft of this report from the Director of FLETC. Generally, FLETC agreed with all of our findings and recommendations. FLETC has developed a remediation plan to address these findings and recommendations. We have incorporated these comments where appropriate and included a copy of the comments at 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, 2008

Appendix A

**Description of Key FLETC Financial Systems and IT Infrastructure
within the Scope of the FY 2008 FLETC Financial Statement Audit**

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008

Below is a description of significant FLETC financial management systems and supporting IT infrastructure included in the scope of the FY 2008 Financial Statement Audit engagement.

Location of Audit: FLETC Headquarters in [redacted] [redacted] and a FLETC field office in [redacted]
[redacted]

Key Systems Subject to Audit:

- [redacted] 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 [redacted]
- [redacted] [redacted] FLETC's procurement management system, which is used for the tracking of procurement activities at various FLETC locations. [redacted] [redacted] is a system used to input requisitions for the acquisition of goods and services. [redacted] [redacted] purpose is to process contractual documents generated by FLETC in support of procurement activities. The system resides on an [redacted] [redacted] and the front-end of the system is integrated with [redacted]

**Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008**

Appendix B

**FY2008 Notices of IT Findings and Recommendations – Federal
Law Enforcement Training Center**

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008

Notices of Findings and Recommendation – Definition of Risk Ratings:

The Notices of Findings and Recommendations (NFR) risk was ranked as High, Medium, and Low** based upon the potential impact that each weakness could have on the DHS component's information technology (IT) general control environment and the integrity of the financial data residing on the DHS component's financial systems, and the pervasiveness of the weakness.

****The risk ratings are provided solely to assist management with prioritization of corrective actions. The risk ratings have no relationship to the definition, or our classification, of a control deficiency as a material weakness or significant deficiency.** The risk ratings, used in this context, are not defined by *Government Auditing Standards*, issued by the Comptroller General of the United States, or the American Institute of Certified Public Accountants (AICPA) Professional Standards, and do not necessarily correlate to a significant deficiency, as defined by the AICPA Standards and reported in our *Independent Auditors' Report* on the FLETC consolidated financial statements, dated March 26, 2009.

Correction of some higher risk findings may help mitigate the severity of lower risk findings, and possibly function as a compensating control. In addition, analysis was conducted collectively on all NFRs to assess connections between individual NFRs, which when joined together, could lead to a control weakness occurring with more likelihood and/or higher impact potential.

High Risk:** A control weakness that is more serious in nature affecting a broader range of financial IT systems, or having a more significant impact on the IT general control environment and /or the integrity of the financial statements as a whole.

Medium Risk:** A control weakness that is less severe in nature, but in conjunction with other IT general control weaknesses identified, may have a significant impact on the IT general control environment and / or the integrity of the financial statements as a whole.

Low Risk:** A control weakness minimal in impact to the IT general control environment and / or the integrity of the financial statements.

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008

Federal Law Enforcement Training Center
FY2008 Information Technology
Notices of Findings and Recommendations – Detail

**Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008**

**Department of Homeland Security
FLETC
FY2008 Information Technology
Notices of Findings and Recommendations – Detail**

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|----------------|---|--|-----------|--------------|--------------|
| FLETC-IT-08-01 | <p>FLETC finalized and approved the Financial Management System Configuration Management Standard Operating Procedures, which detail testing procedures. This prior year condition will be reissued as the weakness has been in place for the majority of the fiscal year.</p> <p>The access group, “ \ [redacted] has modify, read, execute, and write access to the [redacted] application program libraries. We determined that this gives all FLETC domain level users modify, read, execute, and write access to the [redacted] application program libraries.</p> | <p>We recommend that FLETC Ensure that access to the [redacted] program libraries is limited to only the Administrators group.</p> | | X | Medium |

**Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008**

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|----------------|--|---|-----------|--------------|--------------|
| FLETC-IT-08-02 | <p>FLETC finalized and approved the Financial Management System Configuration Management Standard Operating Procedures, which detail testing procedures. This prior year condition will be reissued as the weakness has been in place for the majority of the fiscal year.</p> <p>Due to the decommissioning of the application, we learned that FLETC has not developed policies and procedures for bug fixes and enhancements. This prior year condition will be reissued as the weakness has been in place for the majority of the fiscal year.</p> <p>All FLETC domain level users inappropriately have modify, read, execute, and write access to the [redacted] support files.</p> | <ul style="list-style-type: none"> Continue with the projected plan for decommissioning the [redacted] application. Develop and implement policies and procedures over the configuration management process for [redacted] application level changes; Ensure that access to the [redacted] program libraries is limited to only the Administrators group. | | X | Medium |
| FLETC-IT-08-03 | <p>The installation of [redacted] system software is not currently logged or reviewed by FLETC management.</p> | <p>We recommend that FLETC, upon implementation of the [redacted] system, enable audit logging over the installation of [redacted] system software and ensure that logs are maintained and proactively reviewed by management.</p> | | X | Medium |
| FLETC-IT-08-04 | <p>The SDLC for [redacted] is currently in draft form.</p> | <ol style="list-style-type: none"> Finalize and implement a SDLC methodology guide for [redacted] FLETC Directive and FLETC Manual. Ensure that security planning has been incorporated throughout the life cycle; Ensure that the SDLC methodology is promulgated to all personnel involved in the | | X | Medium |

**Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008**

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|----------------|--|--|-----------|--------------|--------------|
| FLETC-IT-08-05 | <p>We determined that FLETC has begun to implement corrective actions to address the prior year finding; however we learned that FLETC server level and backups are not periodically tested. Additionally, we noted that procedures or a testing schedule are not in place for server level and backups.</p> | <p>design, development, and implementation process of the SDLC methodology. Consistently apply the new CIO Backup SOP and periodically test the server level and backups at least annually in compliance with the DHS Sensitive System Policy Directive 4300A.</p> | | X | Medium |
| FLETC-IT-08-06 | <p>The contingency plan has not been fully tested. We determine that the recovery and resumption procedures were not tested during the table-top test of the contingency plan.</p> | <ul style="list-style-type: none"> Perform corrective action over the Contingency Plan test results and update the plan accordingly. Perform a test over the Contingency Plan, covering all critical phases of the plan, on an annual basis. | | X | Medium |
| FLETC-IT-08-07 | <p>The FLETC Computer Security Operations Center and Computer Security Incident Response Capability SOP, is currently in draft form. Additionally, we noted that incidents are not tracked from inception to resolution in an incident response management system.</p> | <p>No recommendation will be offered as the condition was mitigated during the fiscal year</p> | | X | Medium |
| FLETC-IT-08-08 | <p>We noted that incompatible duties over have not been identified and that the administrator is no longer a procurement approver. However, policies and procedures have not been developed to segregate incompatible duties.</p> | <p>Continue with the projected plan for decommissioning the application.</p> | | X | Low |

**Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter**
September 30, 2008

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|----------------|--|---|-----------|--------------|--------------|
| FLETC-IT-08-09 | <p>We determined that the procedures for granting access to the Telecom Room have not been documented and no user authorization form is used and maintained for access requests.</p> <p>We noted that no documented procedures on re-entry into the facility after an emergency exist. FLETC also advised that all personnel on the Telecom Room access listing and regular visitors to the Telecom Room are provided fire suppression training. However, no supporting documentation was provided to support this effort.</p> | <ul style="list-style-type: none"> • Document access procedures within the Telecom Room Access SOP, including the use of a user authorization form; • Update the Telecom Room Access SOP to include access granting procedures as well as re-entry procedures, and; • Perform training for Telecom Room staff and regular visitors over emergency procedures pertaining, but not limited to fire, water, and alarm procedures. Additionally, formalize this training by retaining documentation that all staff has completed the training. | | X | Low |

**Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008**

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|----------------|---|---|-----------|--------------|--------------|
| FLETC-IT-08-10 | <p>We found that FLETC Manual (FM) 4300: Information Technology System Security Program and Policy, which establishes the policies to be followed when an employee or contractor is separated or terminated, is currently in draft form. Additionally, [redacted] does not require passwords to contain a combination of upper and lower case letters and special characters.</p> | <ul style="list-style-type: none"> Continue with their projected plan for decommissioning the [redacted] application. Additionally, develop and implement procedures over access authorizations for [redacted] Develop and implement procedures to periodically review the list of [redacted] user accounts; Finalize and implement FM 4300: Information Technology System Security Program and Policy, requiring the immediate notification of terminated or transferred users with FLETC IT accounts; Ensure that the [redacted] application requires a password to be a minimum of eight characters in length and contain a combination of alphabetic, numeric, and special characters to be in compliance with the DHS Sensitive System Policy Directive 4300A. | | X | Medium |
| FLETC-IT-08-11 | <p>We determined that the FLETC Directive (FD) 4320: IT System Security Awareness and Training is in draft form.</p> | <p>No recommendation will be offered as the condition was mitigated during the fiscal year.</p> | | X | Low |
| FLETC-IT-08-12 | <p>We determined that FLETC is in the process of refining the FD/FM 4300 to be in accordance with the DHS Sensitive System Policy Directive 4300A.</p> | <p>We recommend that FLETC finalize and update FD/FM 4300 based on the most recent version of the DHS Sensitive System Policy Directive 4300A and implement the policy, which provides policies and procedures over the authorization and use of mobile code technologies.</p> | | X | Low |

**Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter**
September 30, 2008

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|----------------|---|--|-----------|--------------|--------------|
| FLETC-IT-08-13 | We determined that FLETC has developed policies and procedures to proactively monitor sensitive access to system software utilities for [redacted] in the "FM 4300: Information Technology System Security Program and Policy." However, we noted that this policy is in draft form. | Finalize and implement "FM 4300: Information Technology System Security Program and Policy," which provides policies and procedures to proactively monitor sensitive access to system software utilities for [redacted] | | X | Low |
| FLETC-IT-08-14 | We determined that FLETC has developed policies for restricting access to [redacted] system software in the "FM 4300: Information Technology System Security Program and Policy." However, we noted that this policy is in draft form. | Finalize and implement "FM 4300: Information Technology System Security Program and Policy," which provides policies for restricting access to [redacted] system software; | | X | Low |
| FLETC-IT-08-15 | We noted that FLETC has developed policies for the segregation of duties in the, "FM 4300: Information Technology System Security Program and Policy." However, we noted that the policy is currently in draft form. | Finalize and implement the "FM 4300: Information Technology System Security Program and Policy," which provides policies for segregation of duties in Momentum. | | X | Low |
| FLETC-IT-08-16 | We noted that FLETC has developed policies for the use of [redacted] ([redacted]) technologies, "FM 4300: Information Technology System Security Program and Policy." However, we noted that the SOP is currently in draft form. Additionally, we learned that the security inspections have not been applied to all VoIP networks, but is planned with the new Certification and Accreditation (C&A) scheduled in 2008. | <ul style="list-style-type: none"> Continue to finalize and implement the "FM 4300: Information Technology System Security Program and Policy," which provides policies for the use of VoIP technologies; Conduct a security inspection of the [redacted] installations by completing the [redacted] FLETC Security Checklist. | | X | Medium |

**Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008**

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|----------------|--|---|-----------|--------------|--------------|
| FLETC-IT-08-17 | <p>During our FY 2008 review, we determined that the FLETC has established a process where background checks and periodic reinvestigations for all new and existing contractors are performed in a timely manner and that supporting documentation be maintained. However, we noted a weakness in that two outstanding users still had access to the FLETC network. As a result, the FLETC responded immediately and removed both users' access. However, since the risk was present the majority of the fiscal year, this NFR will be reissued without any recommendations</p> <p>We noted that FLETC has developed policies for the review of [redacted] audit logs, "FM 4300: Information Technology System Security Program and Policy." However, we noted that the SOP is currently in draft form. Additionally, we noted that FLETC has continued with the decommissioning of the [redacted] application; however it has not been completed.</p> | <p>No recommendation will be offered since the condition was mitigated during the fiscal year.</p> | | X | Medium |
| FLETC-IT-08-18 | <p>In FY 2008, FLETC stated that no progress has been made on this weakness. FLETC management recommended setting policy to 5 minutes for all users and then to make exceptions as needed for trainers who need it. FLETC management has submitted an exception waiver to DHS to waiver from the DHS Sensitive System Policy Directive 4300A.</p> | <ul style="list-style-type: none"> Finalize and implement "FM 4300: Information Technology System Security Program and Policy," which provides policies for the review of audit logs; Continue with the decommissioning plan of the [redacted] application. | | X | Low |
| FLETC-IT-08-20 | <p>In FY 2008, FLETC stated that no progress has been made on this weakness. FLETC management recommended setting policy to 5 minutes for all users and then to make exceptions as needed for trainers who need it. FLETC management has submitted an exception waiver to DHS to waiver from the DHS Sensitive System Policy Directive 4300A.</p> | <p>We recommend that FLETC configure the FLETC domain level inactivity threshold of the password protected screensaver to five (5) minutes to be in compliance with the DHS Sensitive System Policy Directive 4300A.</p> | | X | Low |

**Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter**
September 30, 2008

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|----------------|--|---|-----------|--------------|--------------|
| FLETC-IT-08-21 | <p>In FY 2008, we noted that FLETC is in the process of finalizing and implementing FM 4300: Information Technology System Security Program and Policy. Therefore, since the recommendation has not been fully addressed, NFR FLETC-IT-07-21 will be re-issued.</p> <p>FLETC does not capture and maintain user access violations in [redacted].</p> <p>We determined that FLETC has established a process which requires that all [redacted] users will only be granted access once the user access form is appropriately completed and subsequently approved by a supervising authority. Since this improvement was not in place for the majority of the fiscal year, the associated weakness will be reissued with no recommendation.</p> <p>We also determined that FLETC has made progress over the usage of prior passwords. The new process follows the DHS standard of eight iterations. Since this improvement was not in place for the majority of the fiscal year, the associated weakness will be reissued with no recommendation.</p> | <p>We recommend that FLETC finalize and implement FM 4300: Information Technology System Security Program and Policy, and promulgate to all necessary users.</p> | | X | Low |
| FLETC-IT-08-22 | <p>Continue with the projected plan for decommissioning the [redacted] application.</p> | <p>Continue with the projected plan for decommissioning the [redacted] application.</p> | | X | Low |
| FLETC-IT-08-23 | <p>In FY 2008, we learned that FLETC has not validated all users for [redacted]. Additionally, FLETC has removed users that no longer have access, but, this process is not being performed consistently. Therefore, since the finding has not been fully addressed, the NFR will be re-issued.</p> | <ul style="list-style-type: none"> Perform a recertification of all [redacted] user access and validate the existing [redacted] user access of individuals who stated they still need [redacted] access; Continue to consistently remove [redacted] user access that is no longer needed. | | X | Low |

**Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008**

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|----------------|---|---|-----------|--------------|--------------|
| FLETC-IT-08-24 | <p>FLETC provided the FLETC Financial Management System Contingency and Disaster Recovery Plan, dated June 18, 2008. However, the contingency plan did not contain evidence to support that the document is stored offsite.</p> | <p>We recommend FLETC ensure that several updated copies of the Contingency Plan is located at the site for use by contingency staff.</p> | | X | Low |
| FLETC-IT-08-25 | <p>During the FY 08 follow-up, we received the finalized SOP 4203 IT Systems Maintenance Management, effective as of April 29, 2008, and 4204 Anti-Virus for Servers, effective as of April 29, 2008. This NFR will be reissued with no recommendation since the condition has existed for the majority of the fiscal year.</p> | <p>As FLETC has effectively implemented the new policies effective April 2008, no recommendation will be offered.</p> | | X | Low |
| FLETC-IT-08-26 | <p>During technical testing, configuration management weaknesses were identified on hosts and databases supporting the System, and applications.</p> | <ul style="list-style-type: none"> • Implement the corrective actions noted in the findings. • Perform periodic scans of the FLETC network environment, including the financial processing environment, for the identification of vulnerabilities, in accordance with NIST Special Publication (SP) 800-42. • Implement corrective actions to mitigate the risks associated with any vulnerabilities identified during periodic scans. | | X | Medium |

**Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008**

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|----------------|---|---|-----------|--------------|--------------|
| FLETC-IT-08-27 | <p>During technical testing, patch management weaknesses were identified on hosts and databases supporting the [redacted] application. The fact that these vendor supplied patches have not been applied in a timely manner could allow a remote attacker to gain unauthorized access on the host or database.</p> | <ul style="list-style-type: none"> Implement the corrective actions noted in the findings. 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. Implement corrective actions to mitigate the risks associated with any vulnerabilities identified during periodic scans. | | X | Medium |
| FLETC-IT-08-29 | <p>In FY 2008, we learned that [redacted] is still in production; however, no backups are being tested. FLETC management stated that [redacted] decommissioning is planned for the first quarter of FY 08, however at the time of the audit, has not been completed.</p> | <p>Continue with the projected plan for decommissioning the [redacted] application</p> | | X | Medium |
| FLETC-IT-08-30 | <p>During FY 2008 testing of controls after [redacted] conversion, we determined that four (4) support contractors and an additional user account used by the support contractor called "Object CORE admin" had superuser access privileges within [redacted]. Based on notification of this weakness, FLETC management responded by removing the access as of September 24, 2008. Therefore, this finding will be issued with no recommendation.</p> | <p>No recommendation will be offered since the weakness was remediated upon notification.</p> | X | | Medium |

**Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008**

| NFR # | Condition | Recommendation | New Issue | Repeat Issue | Risk Rating* |
|----------------|---|--|-----------|--------------|---------------|
| FLETC-IT-08-31 | During FY 2008, we noted that the application will allow “3 unsuccessful attempts” before the user will be locked out of the application. The application will track these security violations into an audit log; however, the FLETC does not perform a periodic review of the log. | We recommend that application system administrators review security and system-related event logs on a periodic basis. | X | | Medium |
| FLETC-IT-08-32 | During FY 2008 testing of controls after conversion, we determined that the segregation of duties controls were not effective. Specifically, we found that the ‘Accountant-1’ role has the ability to create and approve payment vouchers within | <ul style="list-style-type: none"> • Evaluate the access rights for all roles within and separate the duties for the creation and payment of vouchers. • Develop a process to ensure the segregation of duties between the Accountant roles is maintained. | X | | Medium |

*** Risk ratings are only intended to assist management in prioritizing corrective actions. Risk ratings in this context do not correlate to definitions of control deficiencies as identified by the AICPA.**

**Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008**

Appendix C

**Status of Prior Year Notices of Findings and Recommendations And
Comparison To
Current Year Notices of Findings and Recommendations**

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008

| Component | NFR # | Description | Disposition | |
|-----------|----------------|--|-------------|-----------------------|
| | | | Closed | Repeat |
| FLETC | FLETC-IT-07-01 | <p>The Change Control and Configuration Management SOP for all preventative maintenance and patch management over [REDACTED] is currently in draft form. Additionally, the Change Control and Configuration Management SOP does not detail testing procedures.</p> <p>Documented policies and procedures for [REDACTED] bug fixes and enhancements do not exist, including a description for the emergency change process.</p> <p>The access group, “[REDACTED] \ [REDACTED]” has modify, read, execute, and write access to the [REDACTED] application program libraries. We determined that this gives all FLETC domain level users modify, read, execute, and write access to the [REDACTED] application program libraries.</p> | | FLETC-IT-08-01 |
| FLETC | FLETC-IT-07-02 | <p>The Change Control and Configuration Management SOP for all preventative maintenance and patch management over [REDACTED] is currently in draft form. Additionally, the Change Control and Configuration Management SOP does not detail testing procedures.</p> <p>Documented policies and procedures for [REDACTED] bug fixes and enhancements do not exist, including a description for the emergency change process.</p> <p>All FLETC domain level users inappropriately have modify, read, execute, and write access to the [REDACTED] support files.</p> | | FLETC-IT-08-02 |
| FLETC | FLETC-IT-07-03 | The installation of [REDACTED] system software is not currently logged or reviewed by FLETC management. | | FLETC-IT-08-03 |
| FLETC | FLETC-IT-07-04 | The SDLC for [REDACTED] is currently in draft form. | | FLETC-IT-08-04 |
| FLETC | FLETC-IT-07-05 | <p>[REDACTED] server level and [REDACTED] database backups are not periodically tested.</p> <p>Procedures or a testing schedule are not in place for [REDACTED] server level and [REDACTED] database backups.</p> | | FLETC-IT-08-05 |
| FLETC | FLETC-IT-07-06 | The [REDACTED] contingency plan has not been fully tested. We determine that the recovery and resumption procedures were not tested during the table-top test of the [REDACTED] contingency plan. | | FLETC-IT-08-06 |
| FLETC | FLETC-IT-07-07 | <p>FLETC Computer Security Operations Center and Computer Security Incident Response Capability SOP, is currently in draft form.</p> <p>We noted that incidents are not tracked from inception to resolution in an incident response management system.</p> | | FLETC-IT-08-07 |
| FLETC | FLETC- | We noted that incompatible duties over [REDACTED] [REDACTED] have not | | FLETC-IT- |

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008

| | | | Disposition | |
|------------------|----------------|--|--------------------|-----------------------|
| Component | NFR # | Description | Closed | Repeat |
| | IT-07-08 | been identified nor have policies and procedures been developed to segregate incompatible duties. | | 08-08 |
| FLETC | FLETC-IT-07-09 | We determined that FLETC has documented procedures entitled, "Telecom Room Access Standard Operating Procedures", which are currently in draft form. All personnel on the Telecom Room access listing and regular visitors to the Telecom Room will have fire suppression training provided. However, FLETC failed to provide the fire suppression training materials or a listing of individuals who attended the training. | | FLETC-IT-08-09 |
| FLETC | FLETC-IT-07-10 | Procedures over access authorizations and the periodic review of user accounts for [REDACTED] do not exist. FLETC Manual (FM) 4300: Information Technology System Security Program and Policy establishes the policies to be followed when an employee or contractor is separated or terminated, which is currently in draft form. We found that termination SOPs for [REDACTED] and [REDACTED] are currently under development. [REDACTED] does not require passwords to contain a combination of upper and lower case letters and special characters. | | FLETC-IT-08-10 |
| FLETC | FLETC-IT-07-11 | We determined that the FLETC Directive (FD) 43220: IT System Security Awareness and Training is in draft form. | | FLETC-IT-08-11 |
| FLETC | FLETC-IT-07-12 | We determined that FLETC has developed policies and procedures over the authorization and use of mobile code technologies in "FM 4300: Information Technology System Security Program and Policy." However, we noted that this policy is in draft form. | | FLETC-IT-08-12 |
| FLETC | FLETC-IT-07-13 | We determined that FLETC has developed policies and procedures to proactively monitor sensitive access to system software utilities for Momentum in the "FM 4300: Information Technology System Security Program and Policy." However, we noted that this policy is in draft form. | | FLETC-IT-08-13 |
| FLETC | FLETC-IT-07-14 | We determined that FLETC has developed policies for restricting access to [REDACTED] system software in the "FM 4300: Information Technology System Security Program and Policy." However, we noted that this policy is in draft form. We noted that FLETC has developed procedures for restricting access to privileged and sensitive access including [REDACTED] system software in the Logical Access Controls - SOP, which is currently in draft form. | | FLETC-IT-08-14 |
| FLETC | FLETC-IT-07-15 | We noted that FLETC has developed policies for the segregation of duties in the, "FM 4300: Information Technology System Security Program and Policy." However, we noted that the policy is currently in | | FLETC-IT-08-15 |

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008

| | | | Disposition | |
|-----------|----------------|---|-------------|-----------------------|
| Component | NFR # | Description | Closed | Repeat |
| | | draft form. We noted that FLETC has developed procedures for the segregation of duties in the, "Logical Access Controls – SOP", which is currently in draft form. | | |
| FLETC | FLETC-IT-07-16 | We noted that FLETC has developed polices for the use of VOIP technologies, "FM 4300: Information Technology System Security Program and Policy." However, we noted that the SOP is currently in draft form. The [REDACTED] hardening guide and SOP are currently in development and not finalized. We determined that FLETC has not completed a security assessment of the [REDACTED] site's [REDACTED] installation. | | FLETC-IT-08-16 |
| FLETC | FLETC-IT-07-17 | We sampled thirty (30) IT contractors for evidence of background investigations and noted the following: <ul style="list-style-type: none"> • Nine (9) IT contractors did not have evidence that a background investigation was initiated or completed; and • For twelve (12) IT contractors, we were not able to validate if background investigations were initiated or adjudicated, due to a lack of documentation or poor documentation of background investigations initiated. | | FLETC-IT-08-17 |
| FLETC | FLETC-IT-07-18 | We determined that FLETC has developed polices for the review of [REDACTED] audit logs in the, "FM 4300: Information Technology System Security Program and Policy." However, we noted that the policy is currently in draft form. Procedures around the detailed review of audit records do not exist. Audit logs are not maintained for [REDACTED] on an application level. | | FLETC-IT-08-18 |
| FLETC | FLETC-IT-07-20 | We noted that the FLETC [REDACTED] is configured to trigger a domain level password protected screensaver after twenty (20) minutes of inactivity on user workstations, which is not in compliance with the DHS Sensitive System Policy Directive 4300A. | | FLETC-IT-08-20 |
| FLETC | FLETC-IT-07-21 | We noted that FM 4300: Information Technology System Security Program and Policy documents policies for the following areas: <ul style="list-style-type: none"> • Use of cryptographic tools over the FLETC [REDACTED] • Use of wireless technologies; and • Data sharing with external parties outside of FLETC. However, we noted that the policy is currently in draft form. | | FLETC-IT-08-21 |

**Department of Homeland Security
Federal Law Enforcement Training Center**
Information Technology Management Letter
September 30, 2008

| Component | NFR # | Description | Disposition | |
|-----------|----------------|---|-------------|----------------|
| | | | Closed | Repeat |
| FLETC | FLETC-IT-07-22 | <p>The following [redacted] [redacted] access control weaknesses were identified:</p> <ul style="list-style-type: none"> • User access violation information is not maintained on an application level; • All new users (a total of eight) requesting access to [redacted] [redacted] failed to have an authorized access request form. • Password parameters have been configured to permit users to reuse prior passwords after six (6) iterations; and • The [redacted] [redacted] Administrator is not informed of separated employees via Human Resources (HR), thus, terminated employees access is not removed in a timely manner. <p>Upon notification of this issue, FLETC took corrective action and the [redacted] [redacted] Administrator is now on the listing of individuals who are informed when an employee is separated.</p> | | FLETC-IT-08-22 |
| FLETC | FLETC-IT-07-23 | <p>The following [redacted] [redacted] access control weaknesses were identified:</p> <ul style="list-style-type: none"> • Lack of documented procedures to recertify users logical access on a yearly basis; and • Recertification of [redacted] [redacted] users is not performed over all users. | | FLETC-IT-08-23 |
| FLETC | FLETC-IT-07-24 | We noted that copies of the [redacted] [redacted] [redacted] Contingency Plan are not securely stored off-site at the alternate processing facility. | | FLETC-IT-07-24 |
| FLETC | FLETC-IT-07-25 | <p>The following [redacted] and [redacted] [redacted] service continuity weaknesses were identified:</p> <ul style="list-style-type: none"> • FLETC SOP - Anti-Virus Software for Servers is not finalized; and • FLETC SOP - System Maintenance Policy and Procedures is not finalized. | | FLETC-IT-08-25 |
| FLETC | FLETC-IT-07-26 | During technical testing, configuration management weaknesses were identified on hosts and databases supporting the [redacted] [redacted] [redacted] and [redacted] [redacted] applications. | | FLETC-IT-08-26 |
| FLETC | FLETC-IT-07-27 | During technical testing, patch management weaknesses were identified on hosts and databases supporting the [redacted] [redacted] [redacted] and [redacted] [redacted] Desktop application. The fact that these vendor supplied patches have not been applied in a timely manner could allow a remote attacker to gain unauthorized access on the host or database. | | FLETC-IT-08-27 |

**Department of Homeland Security
Federal Law Enforcement Training Center**
Information Technology Management Letter
September 30, 2008

| | | | Disposition | |
|------------------|----------------|--|--------------------|----------------------|
| Component | NFR # | Description | Closed | Repeat |
| FLETC | FLETC-IT-07-28 | We noted that [redacted] and [redacted] server backup tape rotation logs are not consistently maintained. | X | |
| FLETC | FLETC-IT-07-29 | We noted that [redacted] server level and [redacted] database backups are not periodically tested. We noted that procedures or a testing schedule are not in place for [redacted] server level and [redacted] database backups. | | FLET-IT-08-29 |

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008

Appendix D

Management Comments

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008


Federal Law Enforcement Training Center
U. S. Department of Homeland Security
1131 Chapel Crossing Road
Glynn, Georgia 31534



Homeland
Security

MAR 02 2009

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General
Information Technology Audits

FROM: Connie L. Titus 
Director

SUBJECT: Response to Draft - *Information Technology Management Letter for the FY2008 FLETC Financial Statement Audit*

The Federal Law Enforcement Training Center (FLETC) appreciates your efforts, those of your staff and contracted services, in assessing the effectiveness of information technology (IT) general controls for the 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, FY2008 Information Technology Management Letter*. The report indicates the FLETC made minimal progress towards the identified control weaknesses in FY2008. Although the FLETC was not able to correct several prior year control weaknesses early in the reporting period, resulting in a reissuance of those weaknesses, many of the control weaknesses were in fact corrected in FY2008. As a result, these weaknesses were reissued with no recommended corrective actions. Additionally, the majority of the prior year technical weaknesses were also corrected in FY2008 with the implementation of the upgraded financial application and supporting servers/database, and the transition to the new DHS procurement system. The FLETC has documented and is implementing additional corrective actions for the remaining control weaknesses.

The FLETC continues to make positive gains toward improving and enhancing our financial application and overall information technology security posture.

Point of contact for additional information or questions is the FLETC Chief Information Officer, Sandy Peavy, 912-267-2014.

cc: Sandy Peavy, FLETC Chief Information Officer
Alan Titus, FLETC Chief Financial Officer

www.fletc.gov

Department of Homeland Security
Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2008

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff for Operations
Chief of Staff for Policy
Acting General Counsel
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, Policy
Assistant Secretary, Public Affairs
Assistant Secretary, Legislative Affairs
DHS GAO OIG Audit Liaison
Chief Information Officer, Audit Liaison
FLETC Audit Liaison

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) 254-4199, 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.