DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Information Technology Management Letter for the FY 2007 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.

OIG-08-70 **June 2008**

Office of Inspector General

U.S. Department of
Homeland Security
Washington, DC 20528

Homeland
Security

JUN 24 2008

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 (FLETC) financial statement audit as of September 30, 2007. 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-08-53, May 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 2007 financial statements and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated June 2, 2008, and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control or conclusion on compliance with laws and regulations.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope 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

Richard L. Skinner
Inspector General

KPMG

KPMG LLP
2001 M Street, NW
Washington, DC 20036

June 2, 2008

Inspector General
U.S. Department of Homeland Security

Chief Information Officer
U.S. Department of Homeland Security,
Federal Law Enforcement Training Center

Chief Financial Officer
U.S. Department of Homeland Security,
Federal Law Enforcement Training Center

Ladies and Gentlemen:

We were engaged to audit the consolidated balance sheets of the U.S. Department of Homeland Security's (DHS) Federal Law Enforcement Training Center (FLETC) as of September 30, 2007 and 2006, and the related consolidated statement of net cost and changes in net position, and combined statement of budgetary resources for the year ending September 30, 2007 (referred to herein as "financial statements") and have issued our report thereon dated May 12, 2008. In planning and performing our audit of FLETC, we considered FLETC's internal control as a basis for designing our auditing procedures for the purpose of expressing our opinion on the 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. We have not considered internal control since the date of our report.

In connection with our fiscal year 2007 engagement, we considered FLETC's internal control over financial reporting by obtaining an understanding of 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 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 FLETC's internal control.

Our audit of FLETC's financial statements as of and for the year ended September 30, 2007 disclosed the following significant deficiencies and compliance and other matters that are described in our Independent Auditors' Report dated May 12, 2008.

Significant Deficiency Considered to be a Material Weakness

A. Management Review of Upward and Downward Adjustments

Other Significant Deficiencies
B. Environmental Clean up Costs
C. Accounts Payable
D. Financial Systems Security

Compliance Matters

E. Federal Financial Management Improvement Act of 1996 (FFMIA)

We also reported other matters related to compliance with the *Anti-deficiency Act.*

The control deficiencies presented for your consideration in this letter include the significant deficiency presented in our Independent Auditors' Report dated May 12, 2008, Exhibit II, Comment D – Financial Systems Security, included in the FLETC Performance and Accountability Report (PAR) for Fiscal Year (FY) 2007. The significant deficiency described herein has been discussed with the appropriate members of management, or communicated through a Notice of Finding and Recommendation (NFRs) and is intended **For Official Use Only**. Our audit procedures are designed primarily to enable us to form an opinion on the 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 the FLETC organization gained during our audit engagement to make comments and suggestions that are intended to improve internal control or result in other operating efficiencies.

The Table of Contents on the next page identifies each section of the letter. In addition, we have provided a description of key financial systems and information technology infrastructure within the scope of the FY 2007 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.

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

INFORMATION TECHNOLOGY MANAGEMENT LETTER

Table of Contents

Appendices

Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2007

OBJECTIVE, SCOPE AND APPROACH

We performed an audit of the Federal Law Enforcement Training Center (FLETC) general controls in support of the FY 2007 FLETC financial statements audit engagement. The overall objective of our audit was to evaluate the effectiveness of information technology (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, formed the basis of our audit procedures. Further information related to the scope of the FLETC's 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.
- *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.

To complement our general IT controls audit procedures, we also performed technical security testing for key network and system devices. The technical security testing was performed from within select FLETC facilities, and focused on test, development, and production devices that directly support FLETC's financial processing and key general support systems.

In addition to testing FLETC's general control environment, we performed application control tests on a limited number of FLETC's financial systems and applications. The application control testing was performed to assess the controls that support the financial systems' internal controls over the input, processing, and output of financial data and transactions.

- *Application Controls (APC)* - Application controls are the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, or payroll.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

Our audit procedures over IT general controls for FLETC included a review of their 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, 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 2007, we noted that FLETC has made some progress on its weaknesses. However, many of the prior year (PY) Notification of Findings and Recommendations (NFR) could not be closed completely due to the impending [redacted] implementations or policies and procedures that are in draft form. As a result, there were only two (2) PY NFRS closed, twenty (20) reissued NFRs, and nine (9) 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.

IT GENERAL CONTROL FINDINGS BY AREA

Entity-Wide Security Program Planning and Management

During FY 2007, we noted weaknesses in the entity-wide security program planning and management. Specifically, conditions noted that impact FLETC's financial processing are as follows:

- Incidents are not tracked from inception to resolution in an incident response management system.
- Twenty-one (21) out of a sample of thirty (30) FLETC contractors did not have evidence that a background investigation was initiated or completed.

Recommendations:

Entity-wide security program planning and management controls should be in place to establish a framework and continuing cycle of activity to manage security risk, develop security policies, assign responsibilities, and monitor the adequacy of computer security related controls.

We recommend that the FLETC Chief Financial Officer (CFO) and Chief Information Officer (CIO) offices ensure the following corrective actions are implemented:

- Finalize and implement the FLETC Computer Security Operations Center and Computer Security Incident Response Capability Standard Operating Procedures (SOP) to establish procedures in incident response management.
- Establish and implement an incident response tracking mechanism to be in compliance with Department of Homeland Security (DHS) 4300A Sensitive Systems Handbook.
- Perform background checks on all new and existing contractors ensuring that background checks and periodic re-investigations are performed in a timely manner and that supporting documentation be maintained.
- Document the status of ongoing and completed background checks in a central repository with critical details about the investigation documented such as: date investigation was initiated or adjudicated, the type of investigation initiated or adjudicated, risk level of contractors' role, and current status of investigation.

FLETC Management Response:

Recommendation 1: Completed. The FLETC Computer Security Operations Center and Computer Security Incident Response Capability Standard Operating Procedure, CIO-4401, was finalized on November 30, 2007.

Recommendation 2: Concur. FLETC has established a basic tracking capability and is now using the DHS established Incident Response Portal. Additionally, FLETC is implementing a more robust Incident tracking capability as part of an integrated IT Operations managing and tracking application.

Recommendation 3: Concur. FLETC has identified all contractors with IT access and has conducted and\or requested the appropriate background investigation for all existing contractors with IT access. Additionally, FLETC has enhanced their personnel and IT security processes to ensure all new contractors with IT access undergo and\or submit evidence of having previously undergone an appropriate suitability background investigation.

Recommendation 4: Completed. FLETC has enhanced their background investigation system to adequately and clearly capture the recommended information.

Access Controls

During FY 2007, access control weaknesses were identified as a result of the general controls review and vulnerability testing. These are important issues because personnel inside the organization who best understand the organization's systems, applications, and business processes are able to obtain unauthorized access to FLETC data.

We noted the following weaknesses related to access controls that impact FLETC's financial processing:

- The following [redacted] access control weaknesses were identified:
  - No policies and procedures are in place over access authorizations to [redacted] system hosting these applications.
  - No policies and procedures are in place to periodically review the list of [redacted] user accounts.
  - Draft policies and procedures exist regarding immediate notification of [redacted] administrators when users are terminated or transferred.
  - Password configurations for [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.
- SOPs for the use and installation of [redacted] technologies have been documented, but are in draft form. In addition, the draft procedures require a risk assessment and security testing, which have not been conducted.

- Configuration Management weaknesses on [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] were identified. Additionally, the same servers were identified as having excessive access privileges.

Recommendations:

- Continue with the projected plan for decommissioning the [redacted] application and implementing [redacted]. Additionally, develop and implement procedures over access authorizations for Prism, to include password requirements of a minimum of eight characters in length and contain a combination of alphabetic, numeric, and special characters to be in compliance with DHS 4300A Sensitive Systems Handbook password policy.
- Finalize and implement FM 4300: IT System Security Program and Policy, requiring the immediate notification of terminated or transferred users with FLETC IT accounts.
- Finalize and implement SOPs over the removal of terminated and transferred [redacted] users.
- Finalize and implement the "FM 4300: IT System Security Program and Policy," which provides policies for the use of [redacted]
- Finalize and implement the [redacted] hardening guide and hardening SOP.
- Conduct a security inspection of the [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.

<u>FLETC Management Response</u>:

Recommendation 1: Concur. FLETC plans to migrate from the [redacted] application to the [redacted] in August 2008. [redacted] technical architecture and operations is beyond FLETC's direct operational control: however, FLETC will address IT security compliance within the Memorandum of Understanding for FLETC's use of [redacted]. FLETC has developed the Procurement Standard Operating Procedure 08-003 [redacted], which addresses access control requirements for [redacted] and will be modified to later address access control to [redacted].

Recommendation 2: Concur. FLETC has established and implemented an email distribution list for notifying stakeholders when persons terminate or permanently leave the FLETC. Additionally, the requirement for immediate notification and use of the email distribution list process has been updated in the FLETC Manual 4330, User Identification and Authentication Management. The overarching

FLETC Directive 4300 and associated manual establishing the baseline FLETC IT Security Program and policies is planned for final publication in FY 08.

Recommendation 3: Concur. FLETC has established and implemented an email distribution list for notifying stakeholders when persons terminate or permanently leave the FLETC; [redacted] administrators are recipients of the notification emails. Additionally, the requirement for immediate notification and use of the email distribution list process has been updated in the FLETC Manual 4330, User Identification and Authentication Management. FLETC has developed a [redacted] access standard operating procedure, which addresses access control requirements for [redacted] and will be modified to later address access control to the [redacted] and has developed [redacted] standard operating procedures, which address application access control and annual recertification of users.

Recommendation 4: Concur. The overarching FLETC Directive 4300 and associated manual establishing the baseline FLETC IT Security Program and policies is planned for final publication in FY 08. Specific policy on the use of [redacted] technologies is addressed in this publication.

Recommendation 5: Concur. FLETC is developing an IT System hardening standard operating procedure, which contains procedures for ensuing hardening of IT System components and the associated hardening guideline, to include the [redacted] hardening guide.

Recommendation 6: Concur. The FLETC [redacted] is currently undergoing a new system certification and accreditation effort and certification testing is scheduled for late FY08. Completion of the [redacted] Security Checklist will be included in the certification testing.

Recommendation 7: Concur. FLETC has reviewed each detailed vulnerability to determine appropriate operational actions. Vulnerabilities have been either corrected or a plan identified for correction based on operational functions and acceptable risks.

Recommendation 8: Completed. FLETC developed and has implemented a vulnerability scanning and management standard operating procedure, which addresses periodic vulnerability scanning of systems and management and mitigation of the identified technical vulnerabilities.

Application Software Development and Change Control

During FY 2007, we noted weaknesses related to application software development and change control. Specifically, conditions noted that impact FLETC's financial processing are as follows:

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

  - 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 "modify, read, execute, and write" access to the [redacted]

- System Development Life Cycle (SDLC) for [redacted] is not finalized.

Recommendations:

- Develop and implement test plan standards and procedures into the Change Control and Configuration Management – SOP. In addition, FLETC should finalize, approve and implement the Change Control and Configuration Management – SOP.
- Develop and implement policies and procedures over the configuration management process fo[redacted] level changes.
- Ensure that access to the [redacted] is limited to only the Administrators group.
- Continue with the projected plan for decommissioning the [redacted]. Develop and implement policies and procedures over the configuration management process for [redacted] level changes.
- Finalize and implement a SDLC methodology guide for [redacted], FLETC Directive and FLETC Manual, as well as incorporating security planning 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.

FLETC Management Response:

Recommendation 1: Concur. FLETC has developed [redacted] specific standard operating procedures, which address [redacted] application configuration management and testing. Additionally, FLETC has finalized the overarching FLETC Directive, associated manual, and standard operating procedures for IT Change Control and Configuration Management.

Recommendation 2: FLETC has developed [redacted] specific standard operating procedures, which address [redacted] application configuration management and application level changes, testing, and integration to production.

Recommendation 3: Concur. FLETC has successfully restricted access to the majority of [redacted] executable and support files to system and application administrators only; however, the current application versions do require access to select files by standard end users. These files have been identified.

Recommendation 4: Concur. FLETC plans to migrate from the [redacted] in August 2008. [redacted] technical architecture and operations is beyond FLETC's direct operational control; however, FLETC will address IT security compliance within the Memorandum of Understanding for FLETC's use of [redacted].

Recommendation 5: Concur. FLETC is developing a draft FLETC Directive that implements the newly published DHS System Life Cycle Guideline.

Recommendation 6: Concur. FLETC is developing a draft FLETC Directive that implements the newly published DHS System Life Cycle Guideline. Once approved, the Directive and guideline shall be promulgated. FLETC has begun implementing the Guideline for new systems while the Directive is undergoing review and approval.

System Software

During FY 2007, we noted one weakness related to system software. Specifically, the condition noted that impacts FLETC's financial processing is as follows:

- The installation of [redacted] software is not logged or reviewed by FLETC management.

Recommendation:

- Upon implementation of the [redacted], enable audit logging over the installation of [redacted] software and ensure that logs are maintained and proactively reviewed by management.

FLETC Management Response:

Recommendation 1: Concur. FLETC began implementation of a [redacted] in the first quarter FY08. The full system implementation and operation is scheduled for completion in June 2008. Once fully implemented, security audit logs from the [redacted] components will be captured within the [redacted] to include administrator actions such as modifications/updates to [redacted] application files.

Service Continuity

During FY 2007, we noted weaknesses related to service continuity. Specifically, conditions noted that impact FLETC's financial processing are as follows:

- [redacted] are not periodically tested.

- The [redacted] contingency plan has not been fully tested.

Recommendations:

- Develop and implement procedures to periodically test the [redacted] in compliance with DHS 4300A Sensitive Systems Handbook.
- Perform corrective action over the [redacted] contingency plan test results and update the plan accordingly.

- Perform a test over the [redacted] contingency plan, covering all critical phases of the plan, on an annual basis.
- Continue with the projected plan for decommissioning the [redacted]. In addition, develop and implement procedures to periodically test the [redacted] in compliance with DHS 4300A Sensitive Systems Handbook.
- Periodically test the [redacted] at least annually in compliance with DHS 4300A Sensitive Systems Handbook.

FLETC Management Response:

Recommendation 1: Concur. FLETC has developed and approved a standard operating procedure for system backups that include periodic testing of system backup files.

Recommendation 2: Concur. FLETC is currently enhancing the [redacted] and updating a contingency plan.

Recommendation 3: Concur. Specific aspects of the applicable contingency plan have been tested annually. FLETC has scheduled a contingency plan test for FY08 that will test all phases of the plan in accordance with DHS guidelines.

Recommendation 4: Concur. FLETC plans to migrate from the [redacted] in August 2008. [redacted] technical architecture and operations is beyond FLETC's direct operational control; however, FLETC will address IT security compliance within the Memorandum of Understanding for FLETC's use of [redacted].

Recommendation 5: Concur. FLETC plans to migrate from the [redacted] in August 2008. [redacted] technical architecture and operations is beyond FLETC's direct operational control; however, FLETC will address IT security compliance within the Memorandum of Understanding for FLETC's use of [redacted]

Segregation of Duties

We did not identify any IT findings in the area of segregation of duties controls during the FY 2007 Financial Statement Audit Engagement.

Application Control Findings

We did not identify any IT findings in the area of application controls during the FY 2007 Financial Statement Audit Engagement.

Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2007

DESCRIPTION OF FINANCIAL SYSTEMS AND IT INFRASTRUCTURE

Below is a description of significant FLETC financial management systems and supporting IT infrastructure included in the scope of the FY 2007 Financial Statement Audit engagement.

[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 the FLETC is involved are processed by [redacted].

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

Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2007

NFR – Definition of Risk Ratings:

The NFRs were risk ranked as High, Medium, and Low based upon the potential impact that each weakness could have on the FLETC control environment and on the integrity of the financial data residing on the DHS component's financial systems. In addition, analysis was conducted collectively on all the 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 serious in nature to create a potential material misstatement to the financial statements.

Medium Risk: A control weakness, in conjunction with other events, less severe - in nature than a high risk issue, which could lead to a misstatement to the financial statements.

Low Risk: A control weakness minimal in impact to the financial statements.

The risk ratings included in this report are intended solely to assist management in prioritizing its corrective actions.

Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2007

FLETC'S IT NOTICES OF FINDINGS AND RECOMMENDATIONS THAT CONTRIBUTED TO A SIGNIFICANT DEFICIENCY BEING REPORTED OVER FLETC'S FINANCIAL SYSTEMS SECURITY

NFR #	Condition	Recommendation	Risk Rating
FLETC-IT-07-01	[redacted] Management Needs Improvement	Develop and implement test plan standards and procedures into the Change Control and Configuration Management – SOP. In addition, FLETC should finalize, approve and implement the Change Control and Configuration Management – SOP. Furthermore, FLETC should develop and implement policies and procedures over the configuration management process for [redacted] application level changes. Lastly, ensure that access to the [redacted] program libraries is limited to only the Administrators group.	Medium

Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2007

NFR #	Condition	Recommendation	Risk Rating
FLETC-IT-07-02	[redacted] Configuration Management Needs Improvement	Develop and implement test plan standards and procedures into the Change Control and Configuration Management – SOP. In addition, FLETC should finalize, approve, and implement the Change Control and Configuration Management – SOP. Furthermore, 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. Lastly, ensure that access to the [redacted] is limited to only the Administrators group.	Medium
FLETC-IT-07-03	Installation of [redacted] Software is Not Logged or Reviewed	Upon implementation of the [redacted], enable audit logging over the installation of [redacted] software and ensure that logs are maintained and proactively reviewed by management.	Medium
FLETC-IT-07-04	SDLC fo[redacted] Is Not Finalized	Finalize and implement the SDLC methodology guide fo[redacted], FLETC Directive and FLETC Manual, as well as incorporating security planning 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.	Medium

Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2007

NFR #	Condition	Recommendation	Risk Rating
FLETC-IT-07-05	[redacted] Backups Are Not Tested	Develop and implement procedures to periodically test the [redacted] in compliance with DHS 4300A Sensitive Systems Handbook. Periodically test the [redacted] at least annually in compliance with DHS 4300A Sensitive Systems Handbook.	Medium
FLETC-IT-07-06	[redacted] Contingency Plan Testing Is Not Complete	Perform corrective action over the [redacted] Contingency Plan test results and update the plan accordingly. Perform a test over the [redacted] Contingency Plan, covering all critical phases of the plan, on an annual basis.	Medium
FLETC-IT-07-07	Incidents Are Not Tracked In an Incident Response Management System	Finalize and implement the FLETC Computer Security Operations Center and Computer Security Incident Response Capability SOP to establish procedures for incident response management. Establish and implement an incident response tracking mechanism to be in compliance with compliance with DHS 4300A Sensitive Systems Handbook.	Medium
FLETC-IT-07-08	Lack of policies and procedures over incompatible duties within [redacted]	Continue with the projected plan for decommissioning the [redacted] Develop and implement policies and procedures that segregate the documented incompatible duties over [redacted]	Low

Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2007

NFR #	Condition	Recommendation	Risk Rating
FLETC-IT-07-09	[redacted] Access Controls Needs Improvement	Document access procedures within the [redacted] Access SOP, including the use of a user authorization form. In addition, FLETC should finalize and implement the [redacted] Access SOP. Lastly, perform training for [redacted] staff and regular visitors over emergency procedures pertaining, but not limited to fire, water, and alarm procedures. Also, formalize this training by retaining documentation that all staff has completed the training.	Low
FLETC-IT-07-10	[redacted] Access Controls Need Improvement	Continue with their projected plan for decommissioning the [redacted] 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: IT System Security Program and Policy, requiring the immediate notification of terminated or transferred users with FLETC IT accounts. Continue to develop, finalize and implement SOPs over the removal of terminated and transferred [redacted] users. 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 DHS 4300A Sensitive Systems Handbook password policy.	Medium

Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2007

NFR #	Condition	Recommendation	Risk Rating
FLETC-IT-07-11	IT Security Awareness Training Is In Draft Form	Ensure that the FLETC Directive (FD) 43220: IT System Security Awareness and Training is finalized, and enforced by having all new and existing FLETC users and contractors complete the training by May 31 of each year.	Low
FLETC-IT-07-12	Policies and Procedures over Mobile Code Technologies Are Not Developed	Finalize and implement FM 4300: IT System Security Program and Policy, which provides policies and procedures over the authorization and use of mobile code technologies.	Low
FLETC-IT-07-13	Policies and Procedures for Review of [redacted] Audit Logs Are Not Developed	Finalize and implement FM 4300: System Security Program and Policy, which provides policies and procedures to proactively monitor sensitive access to system software utilities for [redacted].	Low
FLETC-IT-07-14	Policies and Procedures for Restricting Access to [redacted] System Software Are Not Developed	Finalize and implement FM 4300: IT System Security Program and Policy, which provides policies for restricting access to [redacted] system software. Finalize and implement the Logical Access Controls – SOP, which provides procedures for restricting access to privileged and sensitive access including [redacted] system software.	Low
FLETC-IT-07-15	Policies and Procedures for Segregating Incompatible Duties In [redacted] Are Not Developed	Finalize and implement the FM 4300: IT System Security Program and Policy, which provides policies for segregation of duties in [redacted]. Finalize and implement the Logical Access Controls – SOP, which provides procedures for the segregation of duties in [redacted]	Low

Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2007

NFR #	Condition	Recommendation	Risk Rating
FLETC-IT-07-16	Policies and Procedures over [redacted] Are Not Developed	Finalize and implement the "FM 4300: IT System Security Program and Policy," which provides policies for the use of [redacted]. Finalize and implement the [redacted] hardening guide and hardening SOP. Conduct a security inspection of the [redacted] installations by completing the FLETC [redacted] Security Checklist.	Medium
FLETC-IT-07-17	Background Investigations for Contractors are Not Consistently Performed	Perform timely background checks on all new and existing contractors and ensure that supporting documentation be maintained. Document the status of ongoing and completed background checks in a central repository with critical details about the investigation documented.	Medium
FLETC-IT-07-18	[redacted] Audit Logs Need Improvement	Finalize and implement FM 4300: IT System Security Program and Policy, which provides policies for the review of audit logs. Continue with the projected plan for decommissioning the [redacted] [redacted] application and ensure that audit logs are maintained to capture actual or attempted unauthorized, unusual or sensitive application or operating system level access to [redacted]	Low
FLETC-IT-07-19	[redacted] Password Configurations Need Improvement	This NFR was issued without a recommendation as it was remediated during the audit period.	Low

Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2007

NFR #	Condition	Recommendation	Risk Rating
FLETC-IT-07-20	Access to [redacted] is Not Effectively Controlled	Configure the [redacted] inactivity threshold of the password protected screensaver to five (5) minutes to be in compliance with DHS 4300A Sensitive Systems Handbook.	Low
FLETC-IT-07-21	FLETC Manual (FM) 4300: IT System Security Program and Policy is not finalized	Finalize and implement FM 4300: IT System Security Program and Policy, and promulgate to all necessary users.	Low
FLETC-IT-07-22	Access Controls Over [redacted] Are Not Effective	Continue with the projected plan for decommissioning the [redacted] [redacted] and ensure that user access violation information is maintained at the [redacted] level. Ensure that [redacted] user access is only granted upon completion of a formal [redacted] User Access Control Form, and evidence of supervisory authorization. Configure [redacted] to permit users to reuse prior passwords after eight (8) iterations.	Low
FLETC-IT-07-23	Lack of procedures for recertifying [redacted] Users	Perform a recertification of all [redacted] user access and validate the existing [redacted] [redacted] user access of individuals who stated they still need [redacted] [redacted] access. Remove [redacted] user access that is no longer needed. Develop and implement procedures around the recertification of all [redacted] user access on an annual basis including verifying the access privileges granted to federal employees and contractors.	Low

Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2007

NFR #	Condition	Recommendation	Risk Rating
FLETC-IT-07-24	[redacted] Contingency Plan Is Not Maintained At The Alternate Processing Site	Ensure that several updated copies of the [redacted] Contingency Plan is located at the [redacted] site for use by contingency staff.	Low
FLETC-IT-07-25	Policies and Procedures Over Anti-Virus Software for Servers and System Maintenance Are Not Finalized	Finalize and implement the FLETC SOP - Anti-Virus Software for Servers. Finalize and implement the FLETC SOP - System Maintenance Policy and Procedures.	Low
FLETC-IT-07-26	Configuration Management Weaknesses on the Procurement [redacted]	Implement the corrective actions identified during the audit vulnerability assessment. 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.	Medium
FLETC-IT-07-27	Patch Management Weaknesses on [redacted]	Implement the corrective actions identified during the audit vulnerability assessment. 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.	Medium

Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2007

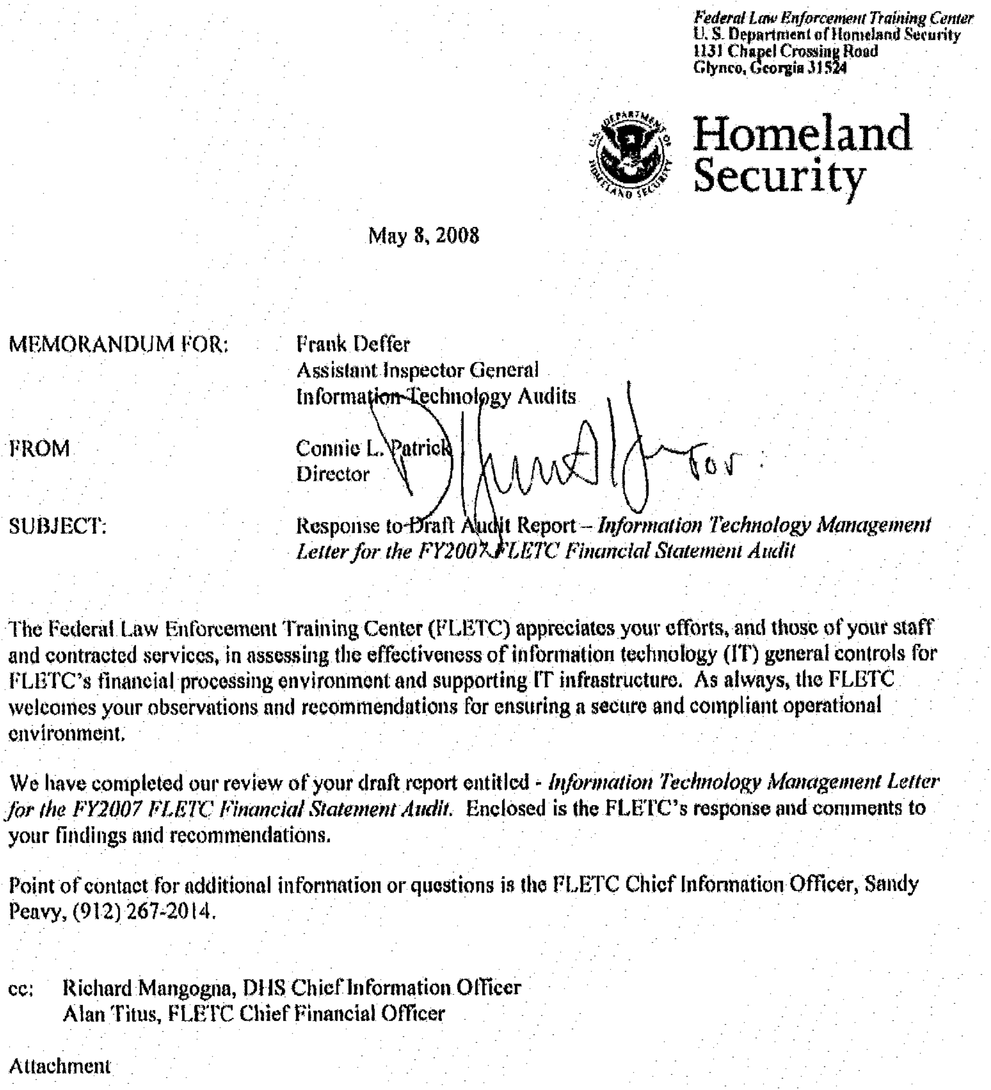
NFR #	Condition	Recommendation	Risk Rating
FLETC-IT-07-28	[redacted] Are Not Consistently Logged	Consistently complete and maintain backup tape rotation logs for [redacted]	Low
FLETC-IT-07-29	[redacted] Are Not Tested	Continue with the projected plan for decommissioning the [redacted] Develop and implement procedures to periodically test the [redacted] in compliance with DHS 4300A Sensitive Systems Handbook. Periodically test the [redacted] at least annually in compliance with DHS 4300A Sensitive Systems Handbook.	Medium

STATUS OF PRIOR YEAR FLETC IT NOTICES OF FINDINGS AND RECOMMENDATIONS

NFR No.	Description	Disposition	
		Closed	Repeat
FLETC-IT-06-01	• No documented configuration management plan is in place for [redacted] including the following: - Lack of documented test plan standards and procedures; - Lack of a documented comprehensive set of test transactions; - Test results are not maintained and a documented approval for the test results does not exist; and - Lack of a description for the emergency change process. • We were unable to verify that an independent control group performed the migration of tested and approved [redacted] system software to the production environment. • We were unable to verify that access to [redacted] program libraries is restricted.		FLETC-IT-07-01
FLETC-IT-06-02	• No documented configuration management plan is in place for [redacted] [redacted], including the following: - Lack of documented test plan standards and procedures; - Lack of a documented comprehensive set of test transactions; - Test results are not maintained and a documented approval for the test results does not exist; and - Lack of a description for the emergency change process. • We were unable to verify that access to [redacted] program libraries is restricted. We noted that a listing of users with access to the [redacted] [redacted] production environment was unavailable.		FLETC-IT-07-02
FLETC-IT-06-03	The installation of [redacted] system software is not logged or reviewed by FLETC management.		FLETC-IT-07-03
FLETC-IT-06-04	The SDLC for [redacted] is currently in draft form.		FLETC-IT-07-04
FLETC-IT-06-05	• [redacted] maintained onsite are not periodically tested. • FLETC does not utilize external labels to indicate the sensitivity of the information on the [redacted] compact discs (CDs).		FLETC-IT-07-05
FLETC-IT-06-06	The [redacted] contingency plan has not been tested.		FLETC-IT-07-06
FLETC-IT-06-07	FLETC Manual 11041: Safeguarding Sensitive But Unclassified (For Official Use Only) Information is currently in draft form and has not been finalized or implemented.	X	
FLETC-IT-06-08	We noted that incidents are not tracked from inception to resolution in an incident response management system.		FLETC-IT-07-07
FLETC-IT-06-09	We noted that there are five (5) generic/shared [redacted] accounts shared amongst the two database administrators (DBAs).		FLETC-IT-07-08

FLETC-IT-06-10	The following [redacted] access control weaknesses were identified: • No policies and procedures are in place to request access to the [redacted]. • No policies and procedures are in place to periodically review the list of persons with physical access to the [redacted] • No emergency policies and procedures are in place for the evacuation and re-entry of the [redacted] • No policies and procedures are in place to guide and document the emergency training of [redacted] personnel.		FLETC-IT-07-09
FLETC-IT-06-11	• No policies and procedures are in place over access authorizations to [redacted] hosting these applications. • No policies and procedures are in place to periodically review the list of [redacted] user accounts. • No policies and procedures are in place to immediately notify [redacted] System administrators when users are terminated or transferred. • Password configurations for [redacted] have been configured to permit passwords to be a minimum of six characters in length with no complexity requirements. • [redacted] users are locked out of the system after five (5) invalid logon.		FLETC-IT-07-10
FLETC-IT-06-12	FLETC Directive (FD) 43220: IT System Security Awareness and Training is currently in draft form and has not been finalized or implemented.		FLETC-IT-07-11
FLETC-IT-06-13	There are no established policies and procedures in place for the authorization and use of mobile code technologies. Currently, FLETC uses [redacted]		FLETC-IT-07-12
FLETC-IT-06-14	There are no policies and procedures in place to review [redacted] audit logs for actual or attempted unauthorized or unusual access to sensitive data.		FLETC-IT-07-13
FLETC-IT-06-15	There are no documented policies and procedures in place for restricting access to [redacted] system software.		FLETC-IT-07-14
FLETC-IT-06-16	Incompatible duties and roles identified within the [redacted] application have not been documented and no policies and procedures exist to segregate incompatible duties and roles.		FLETC-IT-07-15
FLETC-IT-06-17	An established sanctions process for personnel failing to comply with established information security policies and procedures does not exist. However, we noted that FLETC Manual 4900, IT System Rules of Behavior (ROB) and Use Agreements, was finalized in August 2006 and establishes disciplinary actions they could be subject to if the ROB are not followed. We noted that the policy is finalized but has yet to be implemented.	X	
FLETC-IT-06-18	There are no FLETC specific established policies and procedures in place for the use and installation of [redacted]. We noted that FLETC is currently using the Defense Information Systems Agency (DISA) [redacted] Currently, this technology is used at three FLETC sites and is all interconnected through the [redacted] which has a direct connection with [redacted].		FLETC-IT-07-16

FLETC-IT-06-19	We noted that twelve (12) out of a sample of (15) FLETC contractors did not have evidence that a background investigation was initiated or completed.		FLETC-IT-07-17
FLETC-IT-06-20	We noted that a user of the [redacted] has the ability to change the useful life field during the asset entering process.		Issued by the Audit Team
FLETC-IT-06-21	The following [redacted] access control weaknesses were identified: • No policies and procedures are in place to review [redacted] level system software audit logs for successful or unsuccessful access attempts. • No audit logs are maintained to capture actual or attempted unauthorized, unusual or sensitive access within the [redacted] application level.		FLETC-IT-07-18
FLETC-IT-06-22	During technical testing, configuration management weaknesses were identified on the databases supporting the [redacted], as well as supporting servers. Specifically, databases and servers were identified with account management, auditing, database configuration and password management weaknesses.		FLETC-IT-07-26
FLETC-IT-06-23	During technical testing, patch management weaknesses were identified on hosts and databases supporting the [redacted] 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-07-27



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

Homeland
Security

May 8, 2008

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General
Information Technology Audits

FROM Connie L. Patrick
Director

SUBJECT: Response to Draft Audit Report – *Information Technology Management Letter for the FY2007 FLETC Financial Statement Audit*

The Federal Law Enforcement Training Center (FLETC) appreciates your efforts, and those of your staff and contracted services, 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 your draft report entitled - *Information Technology Management Letter for the FY2007 FLETC Financial Statement Audit.* Enclosed is the FLETC's response and comments to your findings and recommendations.

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

cc: Richard Mangogna, DHS Chief Information Officer
Alan Titus, FLETC Chief Financial Officer

Attachment

The Federal Law Enforcement Training Center Response to the Department of Homeland Security, Office of the Inspector General, Draft Audit Report – *Information Technology Management Letter for the FY2007 FLETC Financial Statement Audit*

Responses to Recommendations:

The FLETC concurs with the recommendations of the DHS OIG's audit report and has already taken positive measures to implement or continue implementation of the recommendations. The following comments are provided by finding and recommendation:

Finding 1: Entity-Wide Security Program Planning and Management

Recommendation 1: Finalize and implement the FLETC Computer Security Operations Center and Computer Security Incident Response Capability Standard Operating Procedures (SOP) to establish procedures in incident response management.

FLETC Response: Completed. The FLETC Computer Security Operations Center and Computer Security Incident Response Capability Standard Operating Procedure, CIO-4401, was finalized and implemented on November 30, 2007.

Recommendation 2: Establish and implement an incident response tracking mechanism to be in compliance with Department of Homeland (DHS) 4300A Sensitive Systems Handbook.

FLETC Response: Concur. FLETC has established a basic tracking capability and is now using the DHS established Incident Response Portal. Additionally, FLETC is implementing a more robust Incident tracking capability as part of an integrated IT Operations managing and tracking application.

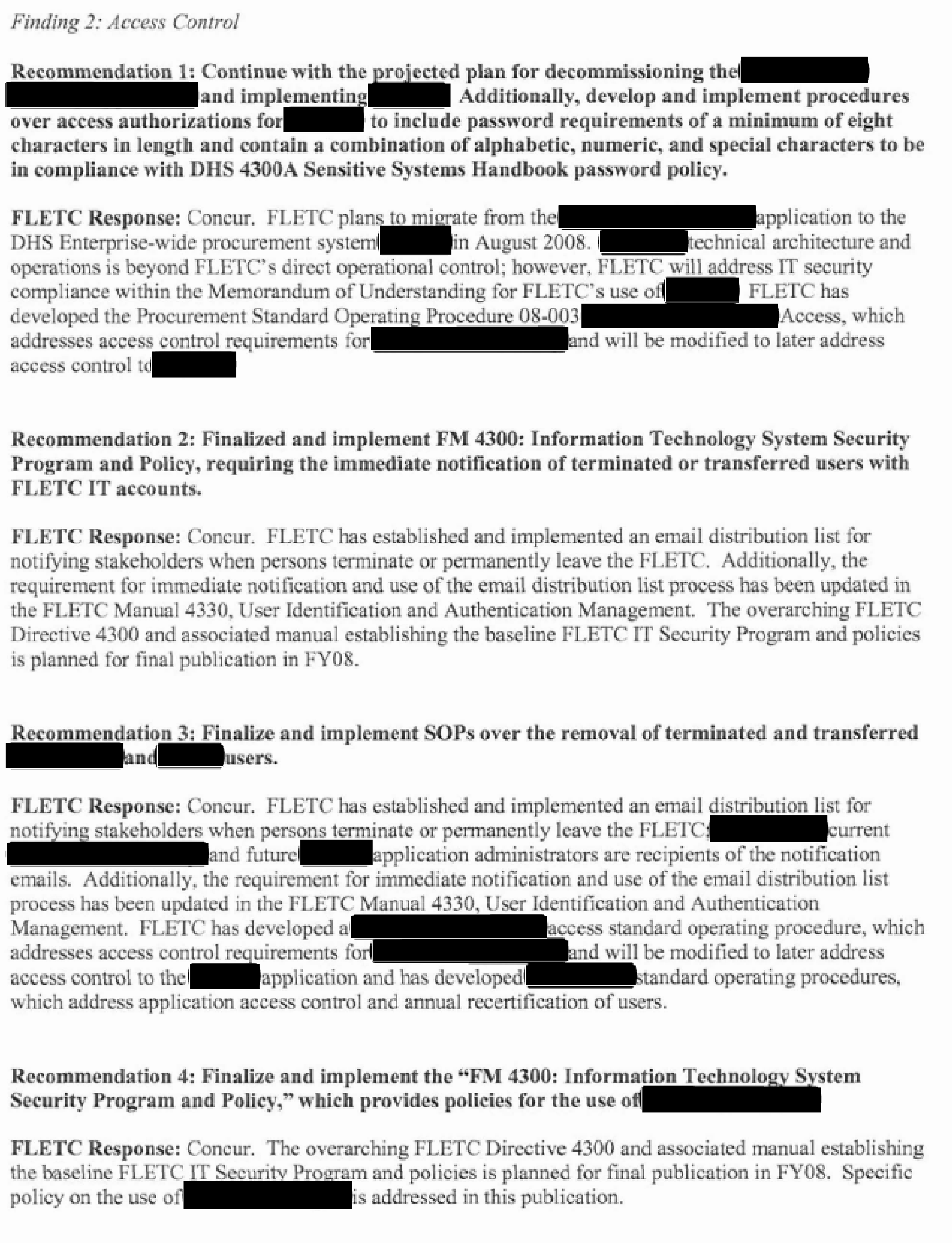
Recommendation 3: Perform background checks on all new and existing contractors ensuring that background checks and periodic re-investigation are performed in a timely manner and that supporting documentation be maintained.

FLETC Response: Concur. FLETC has identified all contractors with IT access and has conducted and/or requested the appropriate background investigation for all existing contractors with IT access. Additionally, FLETC has enhanced their personnel and IT security processes to ensure all new contractors with IT access undergo and/or submit evidence of having previously undergone an appropriate suitability background investigation.

Recommendation 4: Document the status of ongoing and completed background checks in a central repository with critical details about the investigation documented such as: date investigation was initiated or adjudicated, the type of investigation initiated or adjudicated, risk level of contractor's role, and current status of investigation.

FLETC Response: Completed. FLETC has enhanced their background investigation system to adequately and clearly capture the recommended information.

Attachment



Finding 2: Access Control

Recommendation 1: Continue with the projected plan for decommissioning the [redacted] and implementing [redacted] Additionally, develop and implement procedures over access authorizations for [redacted] to include password requirements of a minimum of eight characters in length and contain a combination of alphabetic, numeric, and special characters to be in compliance with DHS 4300A Sensitive Systems Handbook password policy.

FLETC Response: Concur. FLETC plans to migrate from the [redacted] application to the DHS Enterprise-wide procurement system [redacted] in August 2008. [redacted] technical architecture and operations is beyond FLETC's direct operational control; however, FLETC will address IT security compliance within the Memorandum of Understanding for FLETC's use of [redacted] FLETC has developed the Procurement Standard Operating Procedure 08-003 [redacted] Access, which addresses access control requirements for [redacted] and will be modified to later address access control to [redacted]

Recommendation 2: Finalized and implement FM 4300: Information Technology System Security Program and Policy, requiring the immediate notification of terminated or transferred users with FLETC IT accounts.

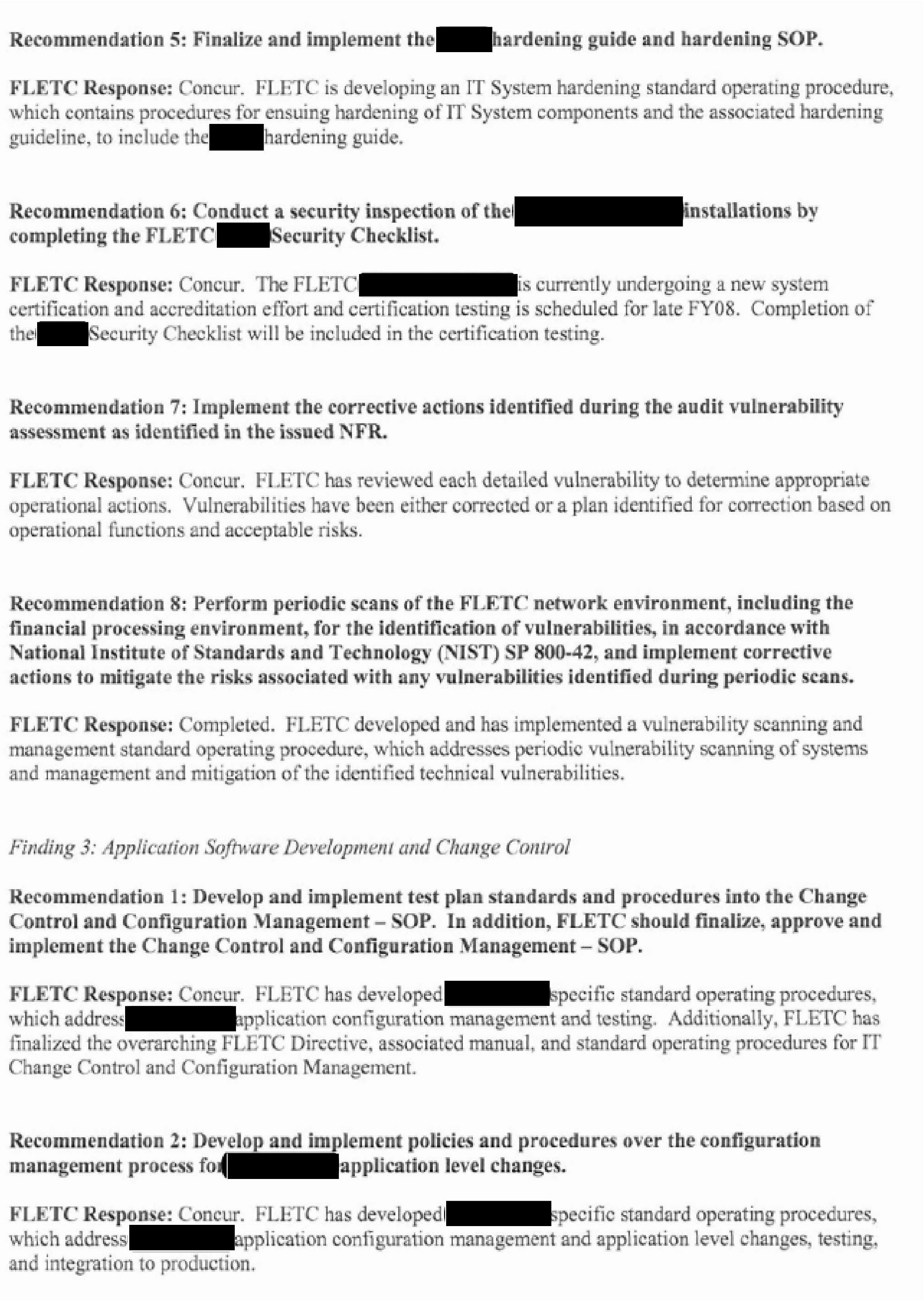
FLETC Response: Concur. FLETC has established and implemented an email distribution list for notifying stakeholders when persons terminate or permanently leave the FLETC. Additionally, the requirement for immediate notification and use of the email distribution list process has been updated in the FLETC Manual 4330, User Identification and Authentication Management. The overarching FLETC Directive 4300 and associated manual establishing the baseline FLETC IT Security Program and policies is planned for final publication in FY08.

Recommendation 3: Finalize and implement SOPs over the removal of terminated and transferred [redacted] and [redacted] users.

FLETC Response: Concur. FLETC has established and implemented an email distribution list for notifying stakeholders when persons terminate or permanently leave the FLETC [redacted] current [redacted] and future [redacted] application administrators are recipients of the notification emails. Additionally, the requirement for immediate notification and use of the email distribution list process has been updated in the FLETC Manual 4330, User Identification and Authentication Management. FLETC has developed a [redacted] access standard operating procedure, which addresses access control requirements for [redacted] and will be modified to later address access control to the [redacted] application and has developed [redacted] standard operating procedures, which address application access control and annual recertification of users.

Recommendation 4: Finalize and implement the "FM 4300: Information Technology System Security Program and Policy," which provides policies for the use of [redacted]

FLETC Response: Concur. The overarching FLETC Directive 4300 and associated manual establishing the baseline FLETC IT Security Program and policies is planned for final publication in FY08. Specific policy on the use of [redacted] is addressed in this publication.



Recommendation 5: Finalize and implement the [redacted] hardening guide and hardening SOP.

FLETC Response: Concur. FLETC is developing an IT System hardening standard operating procedure, which contains procedures for ensuing hardening of IT System components and the associated hardening guideline, to include the [redacted] hardening guide.

Recommendation 6: Conduct a security inspection of the [redacted] installations by completing the FLETC [redacted] Security Checklist.

FLETC Response: Concur. The FLETC [redacted] is currently undergoing a new system certification and accreditation effort and certification testing is scheduled for late FY08. Completion of the [redacted] Security Checklist will be included in the certification testing.

Recommendation 7: Implement the corrective actions identified during the audit vulnerability assessment as identified in the issued NFR.

FLETC Response: Concur. FLETC has reviewed each detailed vulnerability to determine appropriate operational actions. Vulnerabilities have been either corrected or a plan identified for correction based on operational functions and acceptable risks.

Recommendation 8: 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.

FLETC Response: Completed. FLETC developed and has implemented a vulnerability scanning and management standard operating procedure, which addresses periodic vulnerability scanning of systems and management and mitigation of the identified technical vulnerabilities.

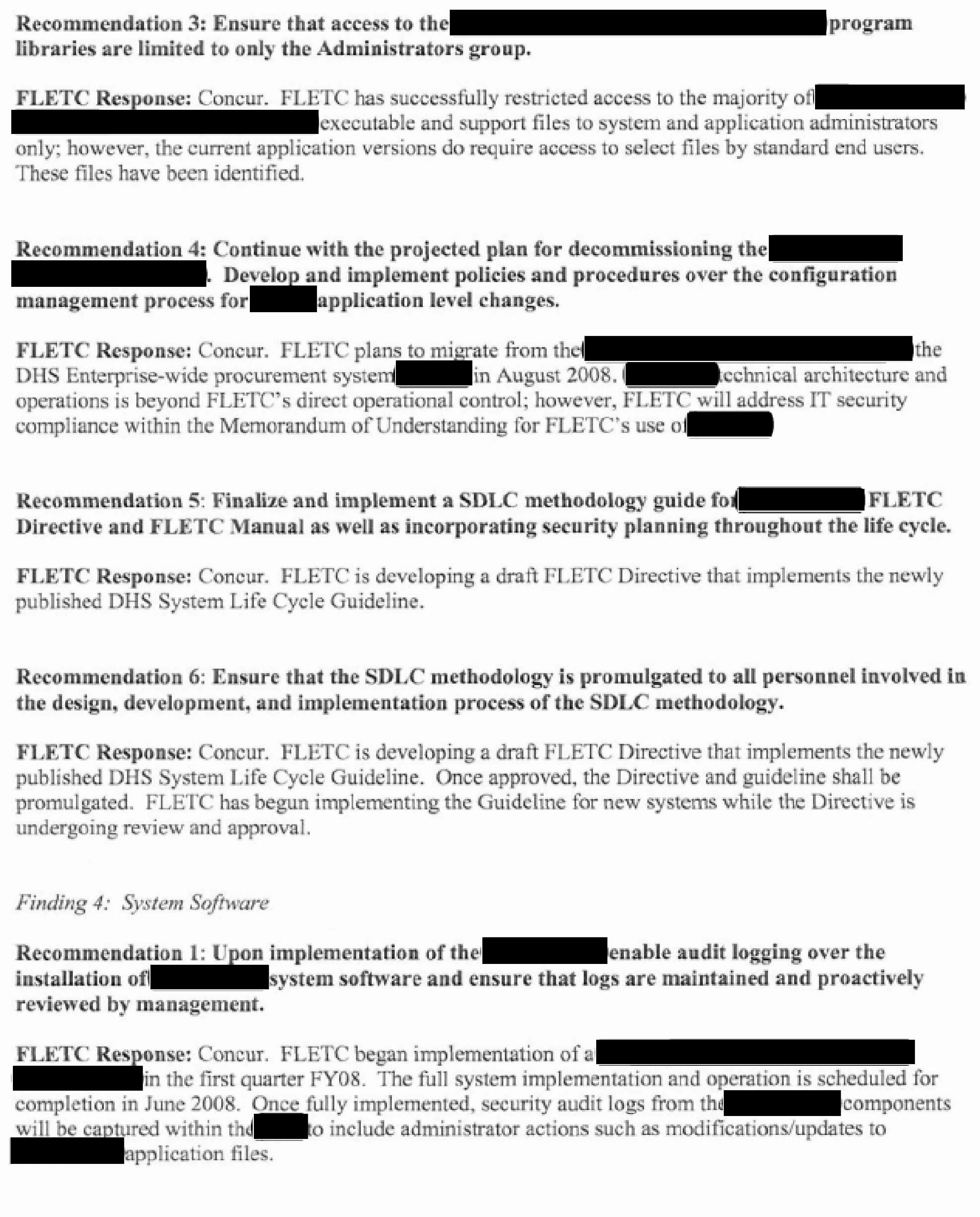
Finding 3: Application Software Development and Change Control

Recommendation 1: Develop and implement test plan standards and procedures into the Change Control and Configuration Management – SOP. In addition, FLETC should finalize, approve and implement the Change Control and Configuration Management – SOP.

FLETC Response: Concur. FLETC has developed [redacted] specific standard operating procedures, which address [redacted] application configuration management and testing. Additionally, FLETC has finalized the overarching FLETC Directive, associated manual, and standard operating procedures for IT Change Control and Configuration Management.

Recommendation 2: Develop and implement policies and procedures over the configuration management process for [redacted] application level changes.

FLETC Response: Concur. FLETC has developed [redacted] specific standard operating procedures, which address [redacted] application configuration management and application level changes, testing, and integration to production.



Recommendation 3: Ensure that access to the [redacted] program libraries are limited to only the Administrators group.

FLETC Response: Concur. FLETC has successfully restricted access to the majority of [redacted] executable and support files to system and application administrators only; however, the current application versions do require access to select files by standard end users. These files have been identified.

Recommendation 4: Continue with the projected plan for decommissioning the [redacted]. Develop and implement policies and procedures over the configuration management process for [redacted] application level changes.

FLETC Response: Concur. FLETC plans to migrate from the [redacted] the DHS Enterprise-wide procurement system [redacted] in August 2008. [redacted]echnical architecture and operations is beyond FLETC's direct operational control; however, FLETC will address IT security compliance within the Memorandum of Understanding for FLETC's use of [redacted]

Recommendation 5: Finalize and implement a SDLC methodology guide for [redacted] FLETC Directive and FLETC Manual as well as incorporating security planning throughout the life cycle.

FLETC Response: Concur. FLETC is developing a draft FLETC Directive that implements the newly published DHS System Life Cycle Guideline.

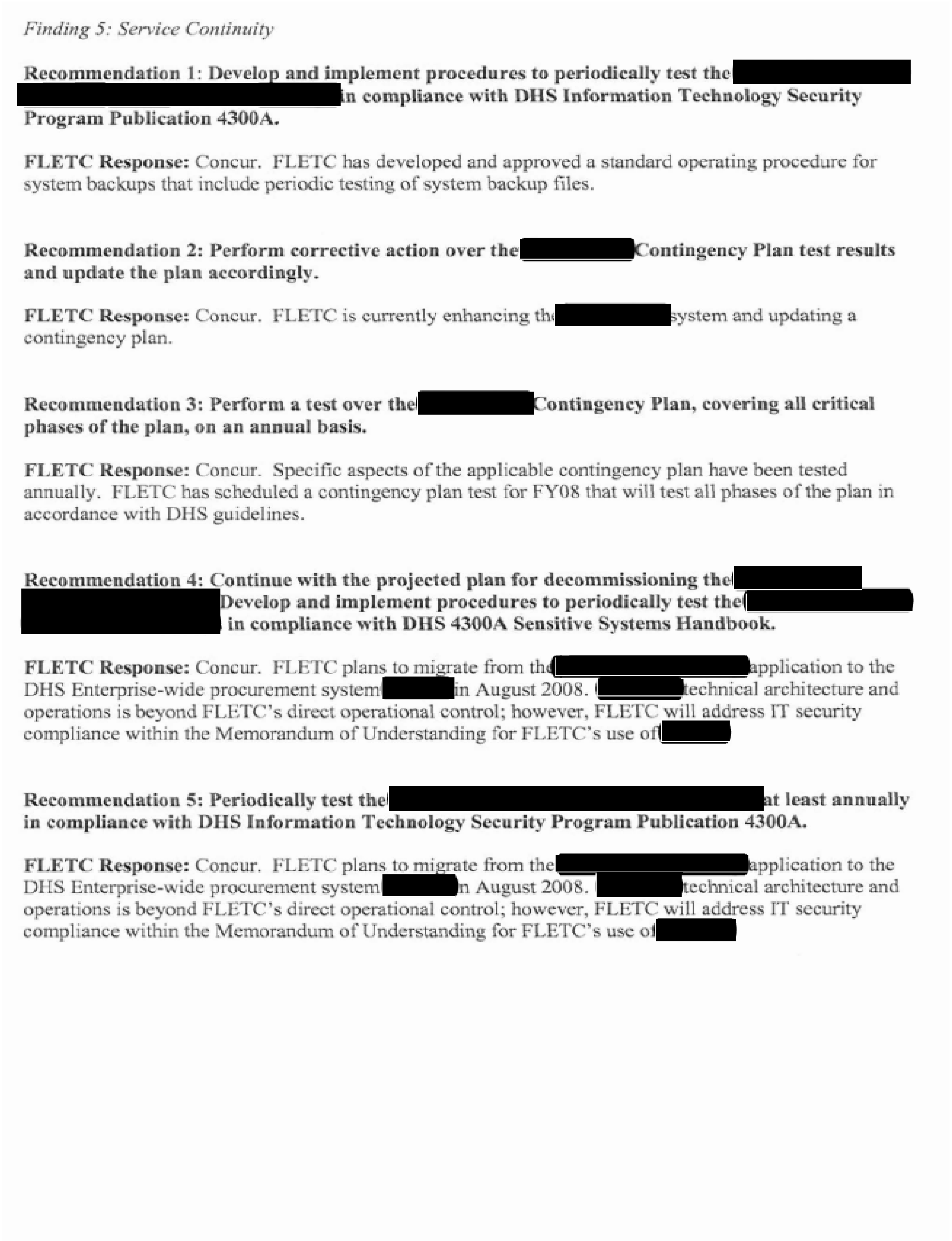
Recommendation 6: Ensure that the SDLC methodology is promulgated to all personnel involved in the design, development, and implementation process of the SDLC methodology.

FLETC Response: Concur. FLETC is developing a draft FLETC Directive that implements the newly published DHS System Life Cycle Guideline. Once approved, the Directive and guideline shall be promulgated. FLETC has begun implementing the Guideline for new systems while the Directive is undergoing review and approval.

Finding 4: System Software

Recommendation 1: Upon implementation of the [redacted] enable audit logging over the installation of [redacted] system software and ensure that logs are maintained and proactively reviewed by management.

FLETC Response: Concur. FLETC began implementation of a [redacted] in the first quarter FY08. The full system implementation and operation is scheduled for completion in June 2008. Once fully implemented, security audit logs from the [redacted] components will be captured within the [redacted] to include administrator actions such as modifications/updates to [redacted] application files.



Finding 5: Service Continuity

Recommendation 1: Develop and implement procedures to periodically test the [redacted] in compliance with DHS Information Technology Security Program Publication 4300A.

FLETC Response: Concur. FLETC has developed and approved a standard operating procedure for system backups that include periodic testing of system backup files.

Recommendation 2: Perform corrective action over the [redacted] Contingency Plan test results and update the plan accordingly.

FLETC Response: Concur. FLETC is currently enhancing th[redacted] system and updating a contingency plan.

Recommendation 3: Perform a test over the [redacted] Contingency Plan, covering all critical phases of the plan, on an annual basis.

FLETC Response: Concur. Specific aspects of the applicable contingency plan have been tested annually. FLETC has scheduled a contingency plan test for FY08 that will test all phases of the plan in accordance with DHS guidelines.

Recommendation 4: Continue with the projected plan for decommissioning the [redacted] Develop and implement procedures to periodically test the [redacted] in compliance with DHS 4300A Sensitive Systems Handbook.

FLETC Response: Concur. FLETC plans to migrate from th[redacted] application to the DHS Enterprise-wide procurement system [redacted] in August 2008. [redacted] technical architecture and operations is beyond FLETC's direct operational control; however, FLETC will address IT security compliance within the Memorandum of Understanding for FLETC's use of [redacted]

Recommendation 5: Periodically test the [redacted] at least annually in compliance with DHS Information Technology Security Program Publication 4300A.

FLETC Response: Concur. FLETC plans to migrate from the [redacted] application to the DHS Enterprise-wide procurement system [redacted] n August 2008. [redacted] technical architecture and operations is beyond FLETC's direct operational control; however, FLETC will address IT security compliance within the Memorandum of Understanding for FLETC's use o[redacted]

Federal Law Enforcement Training Center
Information Technology Management Letter
September 30, 2007

Department of Homeland Security

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