System Application Controls over the Financial Management System

FINAL AUDIT REPORT

ED-OIG/A11J0005
September 2010

Our mission is to promote the efficiency, effectiveness, and integrity of the Department's programs and operations.

U.S Department of Education
Office of Inspector General
Information Technology
Audit Division
Washington, D.C.

NOTICE

Statements that managerial practices need improvements, as well as other conclusions and recommendations in this report represent the opinions of the Office of Inspector General. Determinations of corrective action to be taken will be made by the appropriate Department of Education officials.

In accordance with Freedom of Information Act (5 U.S.C. § 552), reports issued by the Office of Inspector General are available to members of the press and general public to the extent information contained therein is not subject to exemptions in the Act.

Abbreviations/Acronyms Used in this Report

ACS	Affiliated Computer Services, Inc.
CFO	Chief Financial Officer
CIO	Chief Information Officer
COO	Chief Operating Officer
CSO	Chief Security Officer
Department	U.S. Department of Education
FISMA	Federal Information Security Management Act
FMS	Financial Management System
FSA	Federal Student Aid
IA	Information Assurance
IT	Information Technology
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
SP	Special Publication
SSO	System Security Officer
SSP	System Security Plan

UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Information Technology
Audit Division

September 28, 2010

Memorandum

TO: William J. Taggart
Chief Operating Officer
Federal Student Aid

FROM: Charles E. Coe /s/
Assistant Inspector General
Information Technology Audits and Computer Crime Investigations
Office of Inspector General

SUBJECT: Final Audit Report
System Application Controls over the Financial Management System
Control Number ED-OIG/A11J0005

Attached is the subject final audit report that covers the results of our review of system application controls over the Financial Management System for the period August 2007 through July 2009. An electronic copy has been provided to your Audit Liaison Officer. We received your comments generally concurring with the findings and recommendations in our draft report.

Corrective actions proposed (resolution phase) and implemented (closure phase) by your office will be monitored and tracked through the Department's Audit Accountability and Resolution Tracking System (AARTS). ED policy requires that you develop a final corrective action plan (CAP) for our review in the automated system within 30 days of the issuance of this report. The CAP should set forth the specific action items, and targeted completion dates, necessary to implement final corrective actions on the findings and recommendations contained in this final audit report.

In accordance with the Inspector General Act of 1978, as amended, the Office of Inspector General is required to report to Congress twice a year on the audits that remain unresolved after six months from the date of issuance.

In accordance with the Freedom of Information Act (5 U.S.C. § 552), reports issued by the Office of Inspector General are available to members of the press and general public to the extent information contained therein is not subject to exemptions in the Act.

We appreciate the cooperation given us during this review. If you have any questions, please call Therese Campbell at 202-245-7367.

Enclosure

cc: John W. Hurt, III, FSA Chief Financial Officer
Richard J. Gordon, FSA Chief Information Officer
Marge White, FSA Audit Liaison Officer

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Financial Management System (FMS) is an integrated system, utilizing Oracle Federal Financials, which incorporates full financial business functionality, including general ledger, accounts payable, and accounts receivable across multiple Federal Student Aid (FSA) program areas. FMS supports FSA service areas, enterprise areas and partners, and provides timely and consistent financial data for strategic decision making. FMS supports the FSA Chief Financial Officer (CFO) directive to account for all FSA program transactions, performs funds checking, and supports the Department's financial statements. FMS is the single point of institutional financial information for FSA, integrating data from several sources. Accordingly, FMS is the only place within the Department of Education (Department) to obtain a comprehensive financial picture of a school across all FSA programs.

Our original audit objective was to determine whether the Department has effective internal controls over the confidentiality, integrity, and availability of data, and the overall management of the Information Technology (IT) function for FMS. On December 11, 2009, we expanded the scope to include a review of selected IT security controls. During the audit, we learned that source documentation, the original record of a transaction, is not handled or stored by FMS. Instead, this source documentation (including invoices, loan documentation, and receipts) is kept with the source (or feeder) system and sent as a batch by the feeder system for processing (batch processing) to FMS. As a result, we did not evaluate the confidentiality, integrity, and availability of data within FMS due to a lack of source documentation. Our audit covered the period from August 2007 through July 2009.

We found that FSA had adequate safeguards in place over select technical controls for FMS. Specifically, FSA had controls over FMS account management and enforcement, supervision and review over FMS accounts, FMS password policy settings, and monitoring of FMS audit records. FSA also had adequate controls over contractors' work to include complete daily processing activities for FMS, including batch processing of transactions sent by the feeder systems.

However, we found FSA did not have adequate controls in place over personnel security and security and awareness training. FSA also did not ensure adequate physical and environmental controls at a contractor facility.

Personnel Security

FSA did not effectively monitor personnel security clearances and lacked proper procedures to verify clearances for external FMS users.[1] FSA permitted FMS users access to FMS responsibilities that exceeded approved clearance levels. FSA also did not have a policy in place to properly verify security clearance levels of external FMS users.

[1] For this audit, we defined external users as users associated with lenders, servicers, guaranty agencies, and contractors other than Avineon/ACS.

FSA officials acknowledged that in previous years, clearance levels were not thoroughly checked but stated they are now addressing this issue. FSA also stated it had no procedures in place to govern obtaining clearance information for external FMS users. FSA provided evidence that external FMS users did not access FMS directly. External FMS users have access to summary data only and can access data only for their assigned organization. This is a modified repeat finding, also addressed in Audit A11I0002, *IT Security Controls Over the Debt Management Collection Process, Phase I Fiscal Year 2008*, dated September 2008.

These issues occurred because the FMS System Security Officer (SSO) did not properly ensure that users were given responsibilities that were only at or below their approved security clearance level. In addition, FSA officials made a business decision not to obtain and verify the clearances of external users to FMS systems. FSA considered this standard business operating procedure since 2001. By mistakenly granting users access to FMS data at a level it deemed has the potential for serious impact to system data and by choosing to not implement policies and procedures over external FMS users' clearance levels, FSA has potentially left FMS vulnerable to malicious or inexperienced users with unnecessary access to the financial data within.

We recommend that the FSA CFO ensure procedures are in place to verify all users that are granted FMS responsibilities have an approved security level that is at or above the FMS responsibilities they are assigned, develop a policy for SSOs that defines proper procedures for requesting and verifying security clearance information for external FMS users, and request security clearance information from external FMS users in order to verify their security clearance level(s).

Security and Awareness Training

FSA did not ensure that FMS users completed applicable security and awareness training for the 2008 and 2009 training years. Specifically, 2 of 94 FMS users sampled did not take standard security and awareness training in 2008 and 2009, and 10 of 94 FMS users did not take specialized FSA security and awareness training in 2008 and/or 2009. FSA acknowledged that procedures to identify users that required specialized training were not fully in place. By not ensuring that each user is properly trained based on their assigned roles and responsibilities, FSA officials lack the assurance that sensitive data within FMS is properly protected and maintained.

We recommend that the FSA Chief Security Officer (CSO) review the procedures in place used by FSA officials to report users' training to ensure all required training is reported and tracked by the responsible official. Additionally, the CSO should ensure all users with access to FMS take the required standard FSA security and awareness training annually, and ensure FMS users requiring specialized training and any refresher training receive this required training, per Federal guidelines and OCIO's Handbook for Information Assurance Security, to responsibly perform their duties.

Physical and Environmental Controls

FSA did not ensure that a contractor adequately managed all environmental controls for fire prevention at a Germantown, MD facility. During a site visit on July 7, 2009, it was discovered that the contractor facility displayed a lack of proper fire stop materials for core holes drilled between the fifth and sixth floors in telecommunication closets that housed Department assets.

Fire stop is a passive fire protection system of various components used to seal openings and joints in fire-resistance rated wall and/or floor assemblies, based on fire testing and certification listings. Unprotected openings in fire separations allow the spread of fire past the limits of the fire safety plan of the entire building. Fire stop is designed to impede the spread of fire through the opening by filling the openings with fire resistant materials.

Neither FSA nor the contractor provided an explanation for the missing and inadequate fire stop. Penetrations made in fire-rated walls and floors that are left unprotected or improperly protected permit fire, toxic gases, and smoke to travel throughout the building, contaminating many remote areas that would otherwise be unaffected by a fire. Leaving these penetrations unprotected could result in a loss of valuable Department assets and injury.

The inadequate fire stop was addressed by FSA on June 5, 2010. FSA verified, through site inspection, fire stop had been added to the holes in the fifth and sixth floors of the contractor facility. No further recommendation is necessary.

In response to our draft report, FSA thanked the OIG for the extensive effort in support of this audit and concurred with the majority of findings and recommendations identified. FSA was encouraged that OIG's report provides the details that it could use to formulate a comprehensive action plan to address the audit findings and recommendations. FSA was also encouraged that the OIG helped confirm that the FMS has most of its controls in place. FSA stated remediation is already completed or is being worked in several of the cited areas. Additionally, FSA stated that all actions associated with the recommendations in this report will be entered into and tracked through the Department's audit resolution process as part of its Plans of Actions and Milestones (POAM) process. We summarized and responded to specific comments in the "Findings" section of the audit report. FSA's response is included as an enclosure to this audit report.

BACKGROUND

The Financial Management System (FMS) is an integrated financial management system, utilizing Oracle Federal Financials, which incorporates full financial business functionality, including general ledger, accounts payable, and accounts receivable across multiple FSA program areas. FMS supports Federal Student Aid (FSA) service areas, enterprise areas and partners and provides timely and consistent financial data for strategic decision making. In addition, FMS provides FSA with a fully auditable accounting system incorporating appropriate security, controls, and audit trails.

One of the primary objectives of FMS is to provide the necessary interfaces and extensions that are required to be fully operational with other FSA systems. FMS manages the flow of all financial information across all FSA information systems. The core of FMS encompasses interfaces (file transfers of data) from program applications to the Oracle Financials application and the consolidation and centralization of all accounting and financial data into one system for FSA programs. For this reason, interfaces to the FMS application constitute a major portion of the system activity. There are also customized modules or extensions that provide additional functionality to FMS. These extensions allow for the collection of data from financial partners in various FSA programs. FMS, in turn, interfaces with the Department's general ledger and with other systems to provide accounting and payment transactions.

FMS supports the FSA Chief Financial Officer (CFO) directive to account for all FSA program transactions, perform funds checking, and support the Department's financial statements. FMS is the single point of institutional financial information for FSA, integrating data from several sources. Accordingly, FMS provides consolidated data to support key management analysis and is the only place within the Department to obtain a comprehensive financial picture of a school across all FSA programs. FMS also provides a front-end structure to support the operations of various FSA programs through data input forms and processes.

Additionally, FMS has the following extensions, which allow for the collection of data from financial partners in various FSA programs.

- Leveraging Educational Assistance Partnership Program / Special Leveraging Educational Assistance Partnership Program (LEAPP/SLEAPP)
- Lender Application Process (LAP) and Lender Account Receivables (LARS)
- Forms 2000

To assist in processing transactions through FMS, FSA tasked contractors to provide long-term assistance with FMS. The contractors manage overall aspects of FMS operations, including completion of daily processing activities, investigating and correcting processing failures, transmission of data from the FMS general ledger to FMSS, and validating batch data sent to FMSS.

The users of FMS are:

- External Users

- Internal Users
- Systems Administrators
- Database Administrators

AUDIT RESULTS

Our original objective included a review of whether the Department has effective internal controls over the confidentiality, integrity, and availability of data for FMS. We did not evaluate the confidentiality, integrity, and availability of data within FMS due to a lack of source documentation (including invoices, loan documentation, and receipts). Source documentation, the original record of a transaction, is not handled nor stored by FMS. Instead, this source documentation is kept with the feeder system (i.e. DMCS, COD, and DLSS) and sent by the feeder system as a batch file for processing to FMS. We found that FMS is essentially a pass-through system for the Department. As a result, we did not assess the confidentiality, integrity and availability of data within FMS due to this lack of source documents available within FMS.

FSA had adequate safeguards in place over select technical controls for FMS. Specifically, FSA had controls over FMS account management and enforcement, supervision and review over FMS accounts, FMS password policy settings, and monitoring of FMS audit records. FSA also had adequate controls over contractors that complete daily processing activities for FMS, including batch processing of transactions sent by the feeder systems.

However, FSA did not have adequate controls in place over the security awareness and training and personnel security clearances for FMS users and did not ensure adequate physical and environmental controls of a contractor facility. Specifically, we found FSA did not effectively monitor personnel security clearances and lacked proper procedures to verify clearances for external FMS users. FSA also did not ensure that FMS users completed applicable security and awareness training for the 2008 and 2009 training years. The lack of adequate controls over training and clearances potentially left FMS data vulnerable to malicious or inexperienced users with unverified access and inadequate training. During a site visit to a contractor facility, it was discovered that the facility displayed a lack of proper fire stop materials for core holes drilled between the fifth and sixth floors in telecommunication closets that housed Department assets. Before the inadequate fire stop was corrected, this issue left Department assets vulnerable to loss and injury.

In its comments to the draft report, FSA concurred with the majority of findings and recommendations identified. FSA did not concur with issue 1b and recommendation 1.2. The comments are summarized at the end of each finding. The full text of FSA's comments on the draft report is included as an enclosure to the report.

FINDING NO. 1 Federal Student Aid (FSA) Did Not Effectively Monitor Personnel Security Controls (Modified Repeat Finding)

We reviewed the personnel security clearances and associated FMS responsibilities for a sample of 94 internal and external FMS users and found FSA did not effectively monitor personnel security clearances and FSA lacked proper procedures to verify clearances for external FMS users.

Issue 1a-- FMS Responsibilities Exceeded Clearance Levels

FSA permitted FMS users access to responsibilities that exceeded approved clearance levels.[2] We reviewed the FMS User Access Request packages for sampled FMS users, which contained the FMS Table of Responsibilities. This table is used to assign FMS responsibilities[3] to the user. All FMS responsibilities are then assigned a clearance level. We found 9 of 94 users reviewed had FMS responsibilities assigned that were rated a higher clearance level than what was granted or assumed to be granted the user. FSA acknowledged that in previous years, clearance levels were not thoroughly checked.

According to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, PS-2 "Position Categorization" and PS-3 "Personnel Screening," the organization should assign a risk designation to all positions and establish screening criteria for individuals filling those positions. The organization should then screen individuals requiring access to the information system before authorizing access.

OCIO-01, *Handbook for Information Assurance Security Policy*, Section 4.1.1, "Personnel Security and Suitability" and Section 4.1.4, "Access to Sensitive Information," dated March 31, 2006 states:

> All personnel and contractors accessing Department information and information systems shall undergo background screenings…prior to being granted access to the Department systems. All authorized users must be designated with a sensitivity level, based upon the requirements for the protection of information and IT systems for which that position is authorized.
>
> IT systems must be assigned sensitivity levels for information stored, processed, or transmitted. The determination of whether an individual's official duties require access to sensitive information is to be made by the owner of the information. Personnel who are granted access to sensitive information must have appropriate clearances and must acknowledge and accept the Rules of Behavior before being granted access. Non-disclosure requirements/agreements may be included as part of a system's rules of behavior. Personnel with access to sensitive information shall use only approved Department IT systems to process the information and shall not use personally owned equipment.

[2] There are three clearance levels related to FMS responsibilities: 1C (low risk), 5C (moderate risk), and 6C (high risk). High risk positions have the potential for exceptionally serious impact involving duties especially critical to the agency mission, with broad scope and authority, and with major program responsibilities that affect a major computer/ADP system(s). Moderate risk positions have the potential for moderate to serious impact, involving duties of considerable importance to the agency mission, and with significant responsibilities that affect large portions of a computer/ADP system(s). Low risk positions have the potential for limited impact in relation to the agency mission through the use of computer/ADP system(s).

[3] There are over 100 distinct FMS user roles (called responsibilities in Oracle). Each user role is associated with an application (e.g., Oracle Public Sector Payables, Oracle Public Sector Receivables) within FMS. Users may be assigned one or more roles (responsibilities) in the system that provides certain permission sets (e.g., FSA GL Manager, FSA FMS Operations User).

According to the *System Security Plan for the Financial Management System*, Version 2008.2, dated December 2008, FMS uses a Trust Matrix to assign clearance levels to all positions within the FMS organization. The SSP states that the FMS SSO verifies that new FMS users have the required security clearance prior to granting them access to the system.

FMS users had system responsibilities that exceeded their approved clearance levels because the FMS SSO did not provide proper oversight to ensure that users were given only responsibilities that were at or below their approved security clearance level.

Issue 1b-- FSA had No Policy in Place to Verify Clearances for External FMS Users

FSA did not have a policy in place to properly verify the security clearance levels of external FMS users. During our review of clearance levels for sampled users, FSA could not provide support for the clearance levels listed in the FMS User Request packages. FSA officials stated clearances for external FMS users were not verified because they were granted only responsibilities requiring a 1C clearance level. However, we found five[4] of the sampled external FMS users had responsibilities requiring a 5C clearance level.

FSA stated it had no procedures in place to govern obtaining clearance information for external FMS users. When questioned as to how clearance information is verified for external FMS users, FSA stated, "[T]he assumption for external users (e.g. users from Lender/Servicer and Guaranty Agencies) is that they have a security clearance comparable to the 1C or 5C at the institution they work for." FSA officials also stated clearances for external FMS users were not verified because the external users did not access FMS directly. FSA provided evidence that these users have access to summary data only[5] and can access data only for the agency to which they are assigned. The OIG does not agree that these users, even with indirect access to FMS, do not pose a potential for harm to FMS. FSA granted external FMS users access to the system at a level that had the potential for serious impact, which can lead to a compromise of the system from inexperienced or malicious users. FSA ultimately did not verify security clearances for any external FMS users at any clearance level and, therefore, could not provide assurance that any external FMS users had passed a clearance process before system access was granted.

This issue was also addressed in Audit A11I0002, *IT Security Controls over the Debt Management Collection Process, Phase I Fiscal Year 2008*, dated September 2008. In this audit, we found that FSA permitted private collection agency (PCA) contractor personnel to access the Debt Management Collection System (DMCS) before conducting the proper position risk assessments. The FSA SSO stated that FSA did not perform position risk assessments on any PCA duty positions related to system access. OIG recommended the FSA Chief Operating Officer (COO) ensure proper position risk assessments are performed for the PCA contractor personnel prior to granting access to the DMCS.

According to NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, Revision 2, PS-2 "Position Categorization" and PS-3 "Personnel Screening," the organization should assign a risk designation to all positions and establish screening criteria for

[4] These five users are part of the nine users questioned in finding 1a.
[5] The summary data appears to contain no personally identifiable information.

individuals filling those positions. The organization should then screen individuals requiring access to the information system before authorizing access.

As stated in the *System Security Plan for the Financial Management System*, Version 2008.2, dated December 2008, "[T]he FMS SSO verifies that new FMS users have the required security clearance prior to granting them access to the system."

FSA had no established policy to verify clearances of external FMS users because FSA officials considered the practice of not obtaining and verifying clearances of external FMS users as standard business operating procedure since 2001.

All FMS users must be designated at an FMS responsibilities risk level commensurate with the public trust responsibilities and attributes of their position. FMS responsibilities are ranked according to the degree of adverse impact that an unacceptable person could cause on the FMS application and the data. FMS data was vulnerable to malicious users or inexperienced users with unverified access because FSA granted users access at a level that had the potential for serious impact to system data (a 5C FMS responsibility), and did not implement policies and procedures to verify external FMS users' clearance levels.

Recommendations:

We recommend that the FSA CFO:

1.1 Ensure that procedures are in place to verify all users granted FMS responsibilities have an approved security level that is at or above the FMS responsibilities to which they are assigned.

1.2 Revise existing policy for SSOs to include proper procedures for requesting and verifying security clearance information for all external FMS users.

1.3 Request security clearance information from external FMS users in order to verify their security clearance level(s).

FSA's Comments

FSA concurs with issue 1a and recommendations 1.1 and 1.3. FSA does not concur with issue 1b and recommendation 1.2. FSA does not believe a separate policy should be created for external FMS users because external users should be cleared the same way internal users are cleared. FSA uses the following Department policies for personnel clearances: OM:5-101, Contractor Employee Personnel Security Screening; OIG-1, Personnel Security – Suitability Program; and OCIO-01, Education's Handbook for Information Assurance Security Policy, for personnel screening and clearance requirements. FSA also believes that external users should not be differentiated from other users for clearance requirements. There are current policies and procedures in place that FSA uses for requesting and verifying clearance information. FSA uses the Department's policies and FMS has its procedures documented within the FMS System Security Plan (SSP).

OIG Response

OIG agrees that external FMS users should be cleared the same way internal users are cleared. However, users of FMS that are neither Department employees nor contract employees are not covered by the existing FSA personnel security policies. The three policies listed by FSA apply to Department and contract employees. The five external users with a 5C FMS responsibility were from a guaranty agency (GA) and a GA is not under contract with the Department. Therefore, employees of GAs are not covered by the three policies listed. We reviewed the organizational participation agreement between the Department and GAs. This agreement, along with the federal regulations that govern this agreement, does not mandate that GAs provide security clearance data to the Department.

Since external users should be cleared the same way internal users are cleared, the SSP should also cover external users[6] in the procedures related to the verification of security clearance. A review of the October 2009 SSP shows only Department personnel and contractors are addressed.

We reworded recommendation 1.2 to address FSA's choice of modifying its existing policy to include all FMS users instead of creating new policy for external FMS users only.

FINDING NO. 2 FSA Did Not Properly Monitor and Document Security and Awareness Training for FMS Users

FSA did not ensure that FMS users completed applicable security and awareness training for the 2008 and 2009 training years.[7] Specifically, 2[8] of 94 FMS users sampled did not take standard security and awareness training in 2008 and 2009. FMS users with a 6C[9] FMS responsibility are required to take specialized security and awareness training. Ten FMS users[10] did not take specialized FSA security and awareness training in 2008 and/or 2009.

For standard security and awareness training, FSA obtained reports from OCIO online training databases. These reports are then augmented with contractors' offline training. For specialized training, there is no automatically-updated centralized database. All reports are developed from trainee reports, sign-in sheets, completion certificates and other reporting methods to gather the security data. FSA acknowledged that procedures to identify users that required specialized training were not fully in place.

Office of Management and Budget (OMB) Circular A-130, *Security of Federal Automated Information Resources*, Appendix III, dated November 28, 2000, states:

[6] Noted in the October 2009 SSP as external partners.
[7] FSA's training year spans August 1 of one year through July 31 of the next year.
[8] These two users are FSA personnel.
[9] There are three clearance levels related to FMS responsibilities: 1C (low risk), 5C (moderate risk), and 6C (high risk). High risk positions have the potential for exceptionally serious impact involving duties especially critical to the agency mission, with broad scope and authority, and with major program responsibilities that affect a major computer/ADP system(s).
[10] These are FSA employees.

> Before allowing individuals access to the application, ensure that all individuals receive specialized training focused on their responsibilities and the application rules. This may be in addition to the training required for access to a system. Such training may vary from a notification at the time of access (e.g., for members of the public using an information retrieval application) to formal training (e.g., for an employee that works with a high-risk application).
>
> Training is required for all individuals given access to the application, including members of the public. It should vary depending on the type of access allowed and the risk that access represents to the security of the application and information in it. This training will be in addition to that required for access to a support system.

OCIO-01, *Handbook for Information Assurance Security Policy*, Section 4.9, dated March 31, 2006, states:

> A security awareness training program shall be established by the OCIO to ensure all Department personnel and contractors involved in the use of IT systems are aware of their responsibilities for safeguarding the Department's IT resources. All Department personnel, including contractors who have access to the Department's information and information systems that support the operations and assets of the agency, shall fulfill the Department's information system security training program.

As directed by OCIO, the Department's training policy will ensure all personnel and contractors shall complete annual information system security awareness refresher training and information system security personnel with responsibilities related to administering and securing systems are provided with specialized security training applicable to their functions.

According to the *FSA Security Awareness & Specialized Training Process*, dated June 19, 2008, all FSA personnel, contractors, and other users supporting the operations and mission of FSA are required to undergo initial security training and annual security training thereafter to maintain active accounts on FSA information systems. In support of these requirements, the FSA shall also provide specialized or role-based training to all personnel who have significant security responsibilities.

The FSA Training and Awareness Program policy, dated March 2007, describes the roles of FSA officials in the training and awareness program:

> The FSA Chief Security Officer (CSO) is tasked with accomplishing the IT Security Training programs as they apply to FSA employees and contractor employees.
>
> Each System Security Officer (SSO) is tasked as part of his/her duties to apply FSA IT security training policies and procedures to the employees of any contractor supporting his/her system. Among the duties so assigned are collecting information on employees to be trained, directing contractor personnel to take actions to further the programs, and reporting on compliance to the FSA Security & Privacy Team and higher management as needed.

The FSA Security & Privacy Team Training Coordinator is responsible for promulgating information to FSA SSOs, employees, and contractors, and for tracking compliance with the training program through receiving reports from SSOs, FSA managers, employers and contractors. The Training Coordinator is the primary contact between ED CIO/IA, the CSO, SSOs and FSA employees.

Federal agencies and organizations cannot protect the integrity, confidentiality, and availability of information in today's highly networked systems environment without ensuring that all persons involved understand their roles and responsibilities and are adequately trained to perform them prior to being allowed to access systems and sensitive data they may be authorized to use. By not ensuring that each user is properly trained based on assigned roles and responsibilities, FSA officials lack the assurance that sensitive data within FMS is properly protected and maintained.

Recommendations:

We recommend that the FSA CSO:

2.1 Review the procedures in place used by FSA officials to report users' training to ensure all required training is reported and tracked by the responsible official.

2.2 Ensure all users with access to FMS take the required standard FSA security and awareness training annually.

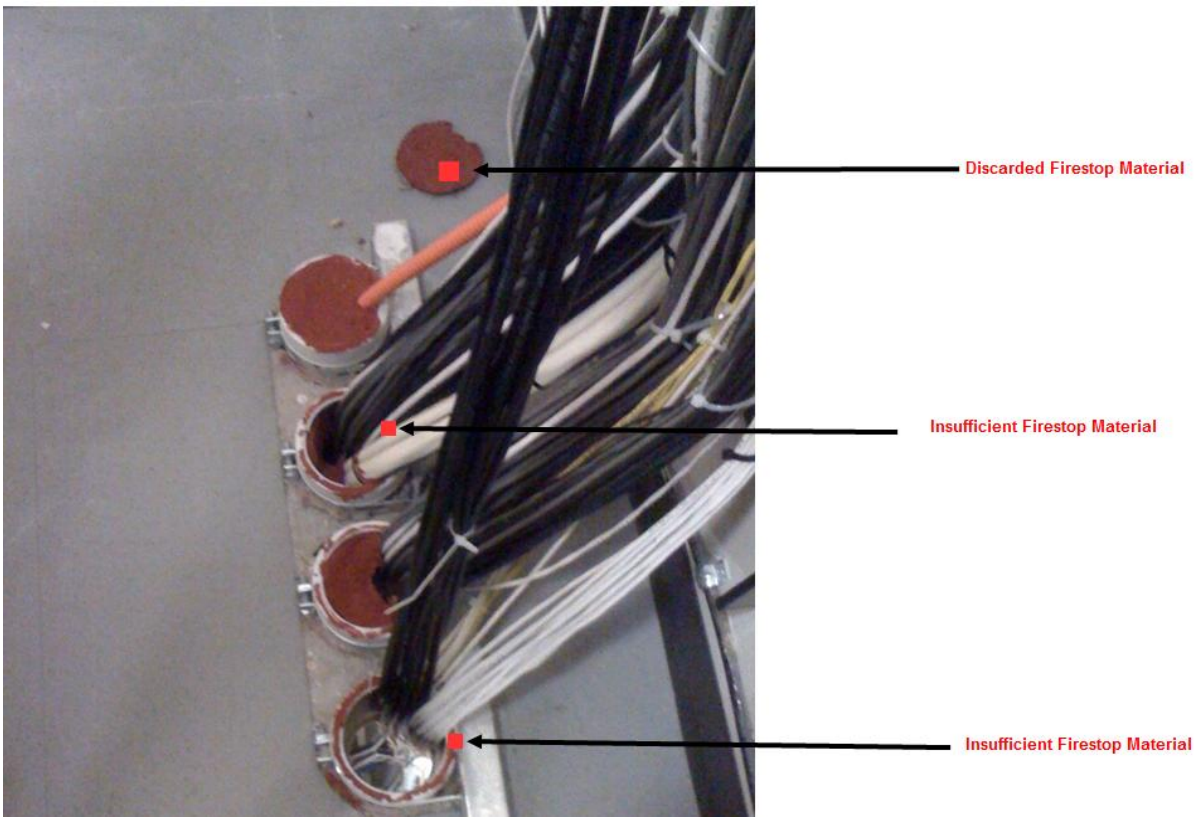
2.3 Ensure FMS users requiring specialized training and any refresher training receive this required training, per Federal guidelines and OCIO's Handbook for Information Assurance Security, to responsibly perform their security-related duties.

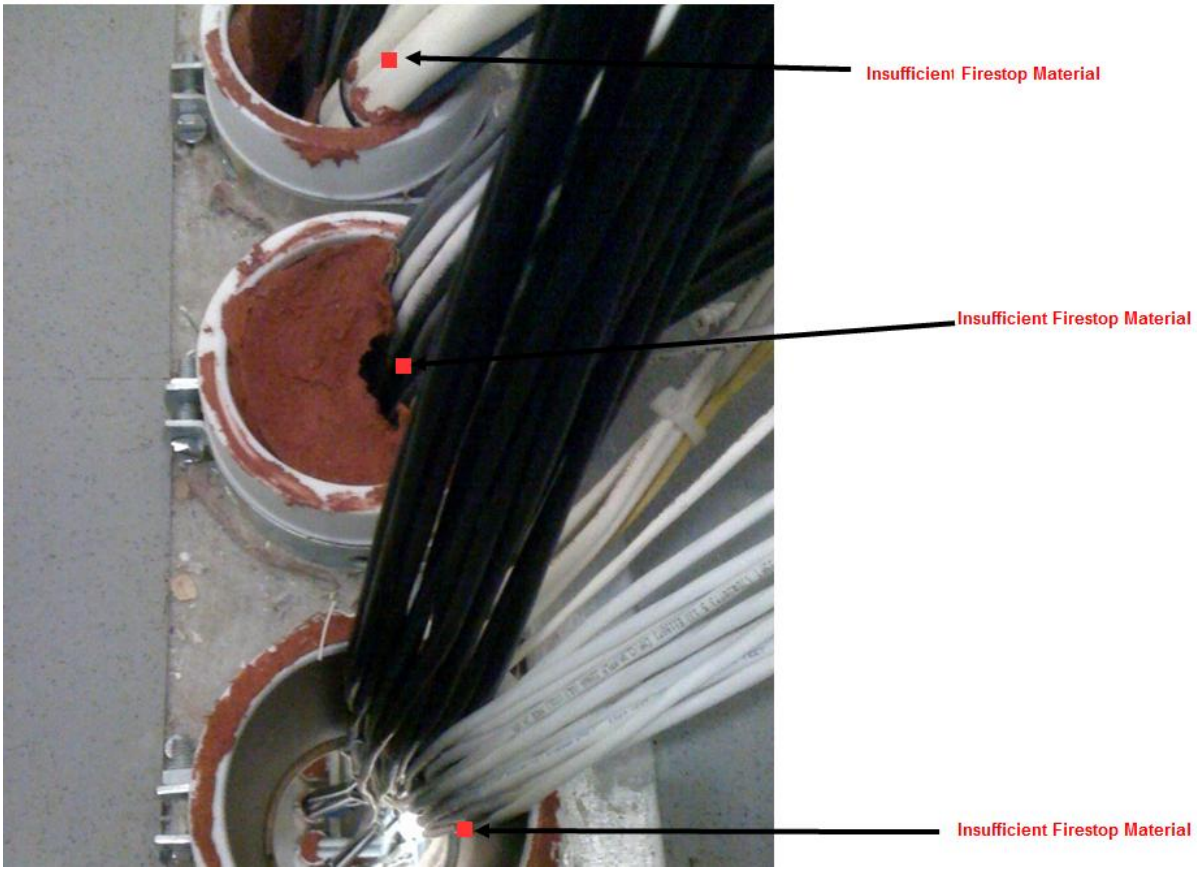
FSA's Comments

FSA concurred with this finding and all recommendations.

FINDING NO. 3 FSA Did Not Ensure that the Contractor Adequately Managed Physical and Environmental Protection of Sensitive Data

FSA did not ensure that Affiliated Computer Services, Inc. (ACS) adequately managed all environmental controls for fire prevention at the Germantown, MD facility. During a site visit on July 7, 2009, it was discovered that the ACS facility displayed a lack of proper fire stop materials for core holes drilled between the fifth and sixth floors in telecommunication closets that housed Department assets.


Discarded Firestop Material
Insufficient Firestop Material
Insufficient Firestop Material


Insufficient Firestop Material
Insufficient Firestop Material
Insufficient Firestop Material

Fire stop is a passive fire protection system of various components used to seal openings and joints in fire-resistance rated wall and/or floor assemblies, based on fire testing and certification listings. Unprotected openings in fire separations void the fire-resistance ratings of the fire separations that contain them, allowing fire to spread past the limits of the fire safety plan of the entire building. Fire stops are designed to restore the fire-resistance ratings of rated wall and/or floor assemblies by impeding the spread of fire through the opening by filling the openings with fire resistant materials.

NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, dated June 2002, states, "IT systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire) from a variety of sources. NIST SP 800-34 recommends that, "Where feasible and cost-effective, preventive methods are preferable to actions that may be necessary to recover the system after a disruption."

The Building Officials and Code Administrators (BOCA) National Building Code of 1996, Chapter 7, *Fire Resistant Materials and Construction,* Section 714.2.3, states, "Where cables, cable trays, conduits, tubes or pipes penetrate a floor assembly, such penetrations shall be protected by a through-penetration fire stop system."

National Fire Protection Association 70, *National Electrical Code,* 1999 Edition, Section 800-52a(2)b, "Installation of Communications Wires, Cables, and Equipment," states, "Installations in hollow spaces, vertical shafts, and ventilation or air handling ducts shall be made so that the possible spread of fire or products of combustion will not be substantially increased. Openings around penetrations through fire resistance-rated walls, partitions, floors or ceilings shall be fire stopped using approved methods."

NFPA 101, *Life Safety Code*, 2000 Edition, Chapter 8.2, "Construction and Compartmentation," Section 8.2.3.2.4.2, states,

> Pipes, conduits, bus ducts, cables, wires, air ducts, pneumatic tubes and ducts, and similar building service equipment that pass through fire barriers shall be protected as follows:
> (1) The space between the penetrating item and the fire barrier shall meet one of the following conditions:
> a. It shall be filled with a material that is capable of maintaining the fire resistance of the fire barrier.
> b. It shall be protected by an approved device that is designed for the specific purpose.

We brought the inadequate fire stop to FSA's attention and it was addressed by FSA on June 5, 2010. FSA verified, through site inspection, fire stop material had been added to the holes in the fifth and sixth floors of the ACS Germantown facility. However, neither FSA nor ACS provided an explanation for the missing and inadequate fire stop. It appears the fire stop was removed due to ongoing maintenance. Evidence of a cable pull (used to thread cable between floors) shows cable was being threaded between the affected floors. Penetrations made in fire-rated walls and floors that are left unprotected or improperly protected permit fire, toxic gases, and smoke to travel throughout the building, contaminating many remote areas that would otherwise be

unaffected by a fire. Leaving these penetrations unprotected could result in a loss of valuable Department assets and injury.

Management Actions Taken

Management corrected the condition on June 5, 2010 and no further recommendation is necessary.

FSA's Comments

The OIG acknowledged that FSA Management corrected the condition on June 5, 2010 and does not have any recommendations for this finding.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our audit objective was to determine whether the Department has effective internal controls over the confidentiality, integrity, and availability of data, and the overall management of the IT function for FMS. On December 11, 2009, we notified FSA that we expanded the scope to include a review of selected IT security controls. We did not evaluate the confidentiality, integrity, and availability of data within FMS due to a lack of source documentation (including invoices, loan documentation, and receipts). Source documentation is kept with the source or feeder system and sent by this feeder system as batch processing to FMS. We found that FMS is essentially a pass-through system for the Department and had no source documentation to review.

Our audit covered the period from August 2007 through July 2009. We conducted our work at the Department's offices in Washington, D.C., and a contractor facility [11] from April 2009 through May 2010. FSA and Department officials declined an exit conference on July 29, 2010.

To accomplish our objectives, we performed the following procedures.

- Reviewed Department policies and procedures and FMS Handbooks and Manuals, comparing these to procedures described in the FMS SSP.
- Interviewed Department officials, including officials with specific roles related to FMS (i.e. SSO, System Owner).
- Interviewed contractor personnel and observed transaction processing at both Department and contractor facilities.
- Obtained a universe of 740 current FMS user accounts active as of May 1, 2008 forward. This universe was then divided into Avineon/ACS contractor users (29), FSA users (60), and external FMS users (651). For this audit, we defined external users as users associated with lenders, servicers, guaranty agencies, and contractors other than Avineon/ACS.
- Obtained a sample of 29 Avineon/ACS contractor users (or 100% of Avineon/ACS users), 25 FSA users, and 25 external FMS users. Our sample size was based on our assessment of FMS risk.
- Reviewed a separate list of 40 high-level users, of which 15 users were evaluated. High-level users are defined as FMS users with system administration access and multiple user capabilities.
- Assessed the sampled FSA, Avineon/ACS, external, and high-level users for adequate security awareness and training, user access and personnel security using hardcopy documentation, including users access forms, rules of behavior, privacy statements, training acknowledgements, Department emails, and user account screen shots from FMS.
- Reviewed and analyzed a separate list of eight users, who initially had access to FMS but left the Department between 5/1/2008 and 4/30/2009, to determine if users had access after the date of separation.

[11] We visited ACS contractor facility in Germantown, MD on July 7, 2009.

- Reviewed a list of 16 FMS users with deactivated accounts to determine if users' had access after the date of deactivation.
- Reviewed and analyzed spreadsheets of FSA standard and specialized security and awareness training for the 2008 and 2009 training years.
- Reviewed and analyzed Oracle and FSA defined database profile settings for FMS passwords.

Use of computer-processed data for the audit was limited to documentation for six FMS transactions provided by FSA. We used the documentation for these six transactions to a limited extent to support FMS' lack of source documents. We did not assess the reliability of the computer-processed data. We used this data for informational purposes only.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Enclosure: Auditee's Comments

September 10, 2010

TO: Charles E. Coe
Assistant Inspector General
Information Technology Audits and Computer Crime Investigations
Office of Inspector General

FROM: John W. Hurt, III /s/
Chief Financial Officer
Federal Student Aid

Richard J. Gordon /s/
Chief Information Officer
Federal Student Aid
(Lead Action Official)

William J. Taggart /s/
Chief Operating Officer
Federal Student Aid

SUBJECT: Draft Audit Report Response
System Application Controls Over the Financial Management System
Control Number ED-OIG/A11J0005

Thank you for the extensive effort in support of the System Application Controls over the Financial Management System (FMS) audit. Federal Student Aid (FSA) concurs with the majority of findings and recommendations identified in the Office of Inspector General (OIG) draft audit report, *System Application Controls over the Financial Management System,* audit control number ED-OIG/A11J0005.

FSA is encouraged that OIG's report provides the details that we can use to formulate a comprehensive action plan to address the audit findings and recommendations. FSA is also encouraged that the OIG has helped us confirm that the FMS has most of its controls in place. FSA concurs with the findings and recommendations identified in the draft report with the following two exceptions:

- FSA does not concur with Issue 1b; *FSA had No Policy in Place to Verify Clearances for External FMS Users*. FSA does not concur that a separate policy should be created for external FMS users because external users should be cleared the same way internal users are cleared. FSA uses the following Department policies for personnel clearances: OM:5-101, Contractor Employee Personnel Security Screening; OIG-1, Personnel Security – Suitability Program; and OCIO-01, Education's Handbook for Information Assurance Policy, for personnel screening and clearance requirements.

- FSA does not concur with recommendation 1.2; *Develop a policy for SSOs that defines proper procedures for requesting and verifying security clearance information for external FMS users*. FSA believes that external users should not be differentiated from other users for clearance requirements. There are current policies and procedures in place that FSA uses for requesting and verifying clearance information. FSA uses the Department's policies and FMS has its procedures documented within the FMS System Security Plan.

Specific responses to the recommendations and details of the OIG report are attached. Remediations are already completed or are being worked in several of the cited areas. Once this report is finalized, our actions associated with your recommendations will be entered into and tracked through the Department's Audit Accountability and Resolution Tracking System (AARTS). Additionally, detailed actions for the findings identified in this report will be tracked until remediated through FSA's Operational Vulnerability Management System (OVMS) as part of its Plans of Actions and Milestones (POAM) process.

Attachment: Federal Student Aid's Response to the System Controls over the Financial Management System

Attachment: Federal Student Aid's Response to the System Application Controls over the Financial Management System
==========

FINDING 1 – Federal Student Aid (FSA) Did Not Effectively Monitor Personnel Security Controls (Modified Repeat Finding)

Issue 1a-- FMS Responsibilities Exceeded Clearance Levels
FSA concurs with this finding issue. *This issue was identified by the FMS ISSO during the annual users renewal process. The cause of the issue resulted from documentation missing from the previous (retired) ISSO and clearance variances between FSA and OM. FSA's initial action was to recertify clearances with the ED/OM during the users annual renewal process. Language was also included in the 2/18/10 annual update of the "Processing FMS User Access Forms & User Recertification Procedures" section 2.1 to recertify renewal clearances and include evidence in the user's access folder. This issue has been resolved through the user's annual renewal cycle and several FMS help desk tickets.*

Issue 1b-- FSA had No Policy in Place to Verify Clearances for External FMS Users
FSA does not concur *that a separate policy should be created for external FMS users because external users should be cleared the same way internal users are cleared. FSA uses the following Department policies for personnel clearances: OM: 5-101, Contractor Employee Personnel Security Screening;, OIG-1, Personnel Security – Suitability Program; and OCIO-01, Education's Handbook for Information Assurance Policy, for personnel screening and clearance requirements.*

Recommendations:
We recommend that the FSA CFO:

1.1 Ensure that procedures are in place to verify all users granted FMS responsibilities have an approved security level that is at or above the FMS responsibilities to which they are assigned.

FSA concurs with this recommendation *and has already updated their annual renewal procedures to revalidate users security level and responsibilities.*

1.2 Develop a policy for SSOs that defines proper procedures for requesting and verifying security clearance information for external FMS users.

- ***FSA does not concur with this recommendation*** *because FSA believes that external users should not be differentiated from other users for clearance requirements. There are current policies and procedures in place that FSA uses for requesting and verifying clearance information. FSA uses the Department's policies and FMS has its procedures documented within the FMS System Security Plan.*

1.3 Request security clearance information from external FMS users in order to verify their security clearance level(s).

FSA concurs with this recommendation *and will conduct a risk-based cost-benefit analysis to determine the feasibility of requesting security clearance information from external FMS users during the annual user renewal process.*

FINDING 2 – FSA Did Not Properly Monitor and Document Security and Awareness Training for FMS Users

FSA concurs with this finding.

Recommendations:
We recommend that the FSA CSO:

2.1 Review the procedures in place used by FSA officials to report users' training to ensure all required training is reported and tracked by the responsible official.

FSA concurs with this recommendation *and will meet with the ED/OCIO IA team responsible for the Department's training procedures to ensure the required training is reported and tracked for FMS users.*

2.2 Ensure all users with access to FMS take the required standard FSA security and awareness training annually.

FSA concurs with this recommendation *and has assigned a staff member to track the Department's Security and Awareness training annually.*

2.3 Ensure FMS users requiring specialized training and any refresher training receive this required training, per Federal guidelines and OCIO's Handbook for Information Assurance Security, to responsibly perform their security-related duties.

FSA concurs with this recommendation *and has assigned a staff member to track the Department's Specialized Security training.*

FINDING 3 – FSA Did Not Ensure that the Contractor Adequately Managed Physical and Environmental Protection of Sensitive Data

Management Actions Taken
The OIG acknowledged that FSA Management corrected the condition on June 5, 2010 and does not have any recommendations for this finding.