

REDACTED

**Security over Certification and Accreditation
for Information Systems**

FINAL AUDIT REPORT



**ED-OIG/A11J0001
October 13, 2009**

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.



UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Information Technology
Audit Division

October 13, 2009

Memorandum

TO: Mr. Tony Miller
Deputy Secretary

Mr. William Taggart
Chief Operating Officer, Federal Student Aid

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

SUBJECT: Final Audit Report
Security over Certification and Accreditation for Information Systems
Control Number ED-OIG/A11J0001

Attached is the subject final audit report that consolidates the results of our review of Security over Certification and Accreditation for Information Systems, A11J0001. An electronic copy has been provided to your Audit Liaison Officer(s). We received your comments mostly concurring with the findings and recommendations in our draft report.

Corrective actions proposed (resolution phase) and implemented (closure phase) by your office(s) 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.

We appreciate the cooperation given us during this review.

Enclosure

TABLE OF CONTENTS

	<u>Page</u>
EXECUTIVE SUMMARY	1
AUDIT RESULTS	4
FINDING NO. 1 - FSA Did Not Properly Review System Security Plans Prior to System Certification and Accreditation	4
FINDING NO. 2 - FSA Did Not Effectively Manage System Interconnection Agreements and Memorandum of Understandings/Agreements.....	7
FINDING NO. 3 - FSA Needs to Improve the Contingency Planning Process	9
FINDING NO. 4 - FSA Needs to Improve Controls over Privacy Impact Assessments for All System Components.....	14
FINDING NO. 5 - FSA Did Not Have Controls in Place to Adequately Manage Authorizations to Operate.....	18
FINDING NO. 6 - FSA Did Not Have Proper Controls in Place to Continuously Monitor System Documentation between C&As.....	21
FINDING NO. 7 - FSA Did Not Properly Conduct Vulnerability Scanning	25
OTHER MATTER- The Department Needs to Update C&A Procedures.....	29
OBJECTIVE, SCOPE, AND METHODOLOGY	30
Enclosure 1: Management Comments.....	32

Abbreviations/Acronyms Used in this Report

AO	Authorizing Official
ATO	Authorization to Operate
BIA	Business Impact Analysis
C&A	Certification and Accreditation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COO	Chief Operating Officer
COS	Continuity of Support Plan
CPS	Central Processing System
Department	U.S. Department of Education
DRP	Disaster Recovery Plan
EDCAPS	Education Central Automated Processing System
EDEN	Education Data Exchange Network
EDSTAR	Education Security Tracking and Reporting System
FISMA	Federal Information Security Management Act
FMS	Financial Management System
FOTW	FAFSA on the Web
FSA	Federal Student Aid
GSS	General Support System
IATO	Interim Authorization to Operate
ISA	Interconnection Security Agreement
IT	Information Technology
MA	Major Application
MOU/A	Memorandum of Understanding or Agreement
NIST	National Institute of Standards and Technology
NSLDS	National Student Loan Data System
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OM	Office of Management
OMB	Office of Management and Budget
OVMS	Operational Vulnerability Management System
PEPS	Postsecondary ED Participants System
PIA	Privacy Impact Assessment
PIN	Personal Identification Number
POA&M	Plan of Action and Milestones
PII	Personally Identifiable Information
SLA	Service Level Agreement
SP	Special Publication
SSO	System Security Officer
SSP	System Security Plan
TPA	Trading Partner Agreement
VDC	Virtual Data Center

EXECUTIVE SUMMARY

The U.S. Department of Education (Department), Federal Student Aid (FSA) manages various Federal student aid programs in its information systems and processes approximately \$69 billion through those systems. The systems manage the financial aspects of student aid and contain substantial amounts of personally identifiable information (PII). The portfolio for the four Major Applications (MAs) and the General Support System (GSS) reviewed were estimated by the Department at over \$108 million for fiscal year 2009.

The Office of Inspector General (OIG) performed a review of the security over the Certification and Accreditation (C&A) process for the Department's information systems. This audit was conducted in accordance with the E-Government Act (Public Law 107-347) including Title III, Federal Information Security Management Act of 2002 (FISMA), and the Privacy Act of 1974. Specifically, we determined whether the Department and FSA properly conducted and supported information systems C&A, and monitored C&A status and updates in accordance with FISMA requirements; National Institute of Standards and Technology (NIST) guidance; and Department and FSA regulations. FISMA requires the OIG to perform independent evaluations on the effectiveness of information security control techniques and to provide assessments of the Department's compliance with the provisions of FISMA.

We evaluated five systems. All of the findings and recommendations in this report refer to these five FSA systems; however, because FSA is a part of the Department, FSA systems contain Department information, and FSA is required to follow Department guidance, the Department's interest could be harmed if FSA does not provide adequate controls over the systems' C&A process. Based on our review, the FSA Chief Operating Officer (COO) and Department Chief Information Officer (CIO) must improve security controls over the C&A process for information systems to adequately protect the confidentiality, integrity, and availability of Department systems and the data residing in the systems.

Phase I - Initiation Phase

- FSA did not properly assess and review system security plans (SSPs) prior to system C&A. Without the proper reviews, FSA officials did not have the most complete, accurate, and trustworthy information possible on the security status of its information systems in order to make timely, and credible, risk-based decisions on whether to authorize operation of those systems. In addition, the Department's C&A packages for four of the systems reviewed were inaccurate because the SSPs were not properly reviewed and updated.
- FSA did not effectively manage system interconnection agreements and memorandum of understandings/agreements. If FSA does not properly monitor the development, management, operation, and security of connections between its interfacing systems, there is a potential for a compromise of all connected systems and the data they store, process, or transmit. It is important that FSA obtains as much information as possible

regarding vulnerabilities associated with its systems to adequately protect Department information.

- FSA needs to improve the contingency planning process for two systems. Because the contingency planning documentation did not include the required Business Impact Analysis (BIA), FSA is not fully prepared for response, continuity, recovery, and resumption of business processes and Information Technology (IT) systems in the event of a disruption. Additionally, the Department's interests could be harmed if the IT contractor does not provide personnel contingency plan training.

Phase II - Security Certification Phase

- FSA needs to improve controls over Privacy Impact Assessments (PIAs). Because FSA obtained authorizations to operate (ATOs) without conducting the proper privacy impact assessments, the Department may be inadequately protecting and handling PII. Sensitive PII could be compromised or damaged, which may lead to identity theft or other fraudulent use of the information.

Phase III - Security Accreditation Phase

- FSA did not have controls in place to adequately manage ATOs. Specifically, FSA continued to operate information systems with an acceptance of risk based on an incorrect accreditation boundary; after significant changes in the operational environment; and after authorizations to operate expired. If the information system is not authorized to operate, further operation should be denied. Without an evaluation of actual changes to the information systems to subsequently determine the impact of changes and risks associated with those changes, authorizing officials did not have the current, correct, and applicable information, conditions, and risks associated with the systems to authorize the systems to operate. Additionally, the system owner must adhere to limitations or restrictions (if any) placed on the operation of the system, based on the ATO.

Phase IV – Continuous Monitoring Phase

- FSA did not have proper controls in place to continuously monitor system documentation between C&As. Without continuously monitoring the security controls of its systems, the Department does not have assurance that the controls remain effective over time in the face of changing threats, missions, environments of operation, and technologies. An effective continuous monitoring program will ensure that important procedures included in the Department's accreditation package are updated as appropriate and contain the necessary information for authorizing officials to make credible, ongoing risk-based decisions regarding the security state of the information systems.
- FSA did not properly conduct vulnerability scanning. It is essential that FSA identify ongoing risks associated with the operation of its systems. FSA cannot adequately protect sensitive information from harm unless it knows the threats and vulnerabilities

associated with its systems. Failure to properly conduct vulnerability scans to identify possible threats and failing to track the effort to correct, reduce, reject, or accept the risks identified by the scans puts the Department at risk of being exploited by potential threats and vulnerabilities.

Other Matter

The Department needs to update C&A procedures. Both the Office of the Chief Information Officer (OCIO) -01 and OCIO-05 Handbooks should be updated to reflect the Office of Management and Budget (OMB) direction regarding unrecognized and unacceptable interim authorizations to operate (IATOs). By allowing IATOs, the Department's systems were operating with identified system security deficiencies and were susceptible to potential threats and vulnerabilities associated with those deficiencies. It is important that security risks and deficiencies are resolved immediately rather than taking months to mitigate those risks, or issuing IATOs. The Department's CIO should review and update the Department's Handbooks to reflect that IATOs are no longer acceptable for authorizations to operate based on the certification and accreditation documentation.

In response to our draft report, FSA and the Department CIO thanked the OIG for the extensive effort undertaken for this audit and concurred with the majority of findings and recommendations identified. FSA stated that one of its highest priorities is ensuring the security of the data it is entrusted to maintain, and that our audit report provided additional insight and direction to ensure this priority is met. The OIG's report provided the details to formulate a comprehensive action plan to address the audit findings and recommendations. We summarized and responded to specific comments in the "Findings" section of the audit report. FSA's and the Department's response is included as Enclosure 1 of this audit report.

FSA stated that some actions resulting from this audit are already completed or being worked. 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.