UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Information Technology Audit Division

September 12, 2011

FINAL MANAGEMENT INFORMATION REPORT

To: James W. Runcie
Acting Chief Operating Officer
Federal Student Aid

From: Charles E. Coe Jr. /s/
Assistant Inspector General for
Information Technology Audits and Computer Crime Investigations

Subject: Survey of Federal Student Aid Contracts and Guaranty Agency Agreements that Provide Information Technology Support or Services
Control Number ED-OIG/X11L0002

The purpose of this **Final Management Information Report** is to provide the U.S. Department of Education (Department), Federal Student Aid (FSA), with information that may strengthen its current contracting process by ensuring that contracts and agreements align with Federal requirements and guidance and with Department and FSA policy and procedures.[1] The objective of our survey was to first identify all FSA contracts providing contractor information technology (IT) support or services[2] to FSA or the Department, as well as all agreements for Guaranty Agencies (GA),[3] which process, store, or transmit Department data through external IT systems as of November 1, 2010. Then, for each FSA contract identified, we determined whether the current contract contained any language that addressed IT security and whether documentation existed to support the certification and accreditation (C&A) of the contractor's system. For each GA agreement identified, we determined whether the current agreement contained any language that addressed IT security.

We found that (1) 7 of the 38 IT support or service contracts reviewed did not contain any language to address IT security; (2) 29 of the 38 contracts reviewed that were subject to the C&A process did not contain all of the documents required to support system C&A; and (3) none of the agreements between FSA and the 32 GAs contained any language that addressed IT security.

[1] To include the E-Government Act (Public Law 107-347), security standards, and guidance issued by the National Institute of Standards and Technology, Office of Management and Budget policy, the Federal Acquisition Regulation, and the Privacy Act of 1974.
[2] IT support services includes the processing, storing, or transmission of data.
[3] A Guaranty Agency is a public or private nonprofit entity that, consistent with 34 Code of Federal Regulations (C.F.R.) §§ 682.400 et seq., performs certain administrative functions in the Federal Family Education Loan Program to provide loan guarantees on loans made by private lenders and collecting or helping rehabilitate defaulted student loans.

BACKGROUND

The Department is obligated to ensure appropriate IT security for operations and assets of the agency. IT security requirements are outlined in Federal requirements and guidance such as the Federal Information Security Management Act of 2002 (FISMA)[4] and publications issued by the National Institute of Standards and Technology (NIST). When dealing with external entities, the Department furthers this obligation through formal agreements and contracts with these entities.

FISMA requires that each Federal agency develop, document, and implement an agency-wide program providing security for the information and information systems that support the operations and assets of the agency. This support also includes operations and assets provided or managed by another agency, contractor, or other source.

NIST, through its Computer Security Division, provides standards and technology to protect information systems against threats to the confidentiality of information, integrity of information and processes, and availability of information and services. These standards include Federal Information Processing Standards[5] (FIPS) Publications and Special Publications[6] (SP).

NIST FIPS Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," dated March 2006, specifies minimum security requirements for information and information systems supporting the executive agencies of the Federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements. Two areas that specifically relate to the scope of this survey include (1) certification, accreditation, and security assessments, and (2) systems and services acquisition.

NIST SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems," dated February 2010, establishes a common information security framework for the Federal government and its contractors.[7] Appendix I of NIST SP 800-37, Revision 1, states that security requirements for external providers, including the security controls for information systems processing, storing, or transmitting of Federal information, are expressed in appropriate contracts or other formal agreements. Appendix I also states that

[4] Enacted as Title III of the E-Government Act (Public Law 107-347), December 2002.
[5] FIPS Publications are issued by NIST after approval by the Secretary of Commerce pursuant to Section 5131 of the IT Reform Act of 1996 (Public Law 104-106) and FISMA. With the passage of FISMA, there is no longer a statutory provision to allow for agencies to waive mandatory FIPS.
[6] Special Publications present documents of general interest to the computer security community. The SP 800 series provides information on NIST's Information Technology Laboratory's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.
[7] Revision 1 redefined the traditional C&A process into a six-step Risk Management Framework. It replaced the May 2004 version titled "Guide for the Security Certification and Accreditation of Federal Information Systems," which defined the security accreditation package as containing a System Security Plan, Security Assessment Report, and Plan of Action and Milestones.

FISMA and Office of Management and Budget (OMB) policy require external providers of information system services handling Federal information or operating information systems on behalf of the Federal government to meet the same security requirements as Federal agencies.

The SP 800-37 Risk Management Framework further states that common control providers[8] are responsible for:

- Documenting the common controls in a system security plan (SSP);
- Ensuring that required assessments of common controls are carried out by qualified assessors with an appropriate level of independence defined by the organization;
- Documenting assessment findings in a security assessment report (SAR); and
- Producing a Plan of Action and Milestones (POA&M) for all controls having weaknesses or deficiencies.

Department of Education OCIO-01 "Handbook for Information Assurance Security Policy," dated March 31, 2006, establishes policies required to comply with Federal laws and regulations, thus ensuring adequate protection of Department IT resources. Additionally, OCIO-05 "Handbook for Information Technology Security Certification and Accreditation Procedures," dated March 31, 2006, establishes a comprehensive and uniform approach to the C&A process for agency systems. The handbooks are consistent with government-wide policies, standards, and procedures issued by OMB, NIST, the General Services Administration, and the Office of Personnel Management.

OBSERVATIONS

With respect to the scope of our review, we determined that 38 active FSA contracts were related to contractor-provided IT support or services. Of those 38 contracts, 7 of the contracts did not address IT security. In addition, 29 of the 38 contracts that were subject to the C&A process did not contain all of the required supporting documentation to verify that the contractor's system was properly certified and accredited in accordance with Federal mandates. We also determined that none of the GA agreements addressed IT security.

Review of Contracts for IT Security Requirements

At the beginning of our survey work, FSA identified a total universe of 241 active contracts. Of the 241 contracts, FSA identified that 52 of these active contracts were related to contractor-provided IT support or services. For all 52 contracts, we verified which contracts were indeed related to contractor-provided IT support or services. Initially, we could not identify the systems that were going to be used in performing the work specified in some of the contracts because

[8] A common control provider is an organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls that are inherited by one or more organizational systems).

they were not specifically identified within the contracts. Therefore, we performed extensive research to determine whether the systems were correctly identified for each contract.

We determined that 4 of the 52 contracts identified by FSA did not provide contractor IT support or services and, therefore, were excluded from our review. Four more of those 52 contracts were multiple contracts for the same system associated with the same contractor and were also excluded from our review. An FSA official identified 6 contracts for which the contractor did not use a system and, therefore, the contract was not subject to the C&A process. Of the remaining 38 contracts, we identified 7 contracts that included no provisions to address IT security. These seven contracts provided services such as processing and disbursement of Direct Loans and Federal Pell Grants; collecting enrollment data for Teacher Education Assistance for College and Higher Education Grant recipients, Direct Loan borrowers, and Department-held Federal Family Education Loan (FFEL) borrowers; managing student aid obligations made under Title IV of the Higher Education Act of 1965, as amended; and providing operation, maintenance, and development services for the Ombudsman Case Tracking System, as well as Ombudsman Web sites.

By not addressing IT security requirements in all IT support and service contracts and agreements, FSA may have insufficient assurances that systems and data, such as personally identifiable information[9] (PII), are protected from unauthorized access, use, disclosure, modification, or destruction.

Certification and Accreditation Support for Contractor Systems

As part of our survey, we also determined whether documentation existed to verify that the contractors' systems were properly certified and accredited consistent with NIST and Department policies.

To conduct our review, we were provided access to the Operational Vulnerability Management System (OVMS) and to FSA public folders within Microsoft Outlook, which an FSA official said contained the C&A documentation for all Departmental systems. After reviewing the documentation in OVMS and Microsoft Outlook, we determined that for 29 of the 38 contracts containing systems that were subject to the C&A process, FSA did not maintain all required documentation. Specifically, we found that:

- 1 contract (3 percent) FSA did not maintain an SSP, SAR, and POA&M;
- 3 contracts (8 percent) FSA did not maintain a SAR and POA&M;
- 9 contracts (24 percent) FSA did not maintain a SAR; and
- 16 contracts (42 percent) FSA did not maintain a POA&M.

[9] PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Changes to an IT system or associated IT environment can affect the accredited safeguards and may result in changes to the prescribed security requirements needed for the system. Therefore, having the appropriate required documentation will help ensure that authorizing officials make credible on-going risk-based decisions regarding the security state of the information systems.

Review of GA Agreements for IT Security Language

As part of our survey work, we requested FSA to provide all GA agreements. As previously noted, GAs process, store or transmit Department data through external IT systems. FSA identified and provided agreements between itself and 32 GAs participating in the FFEL Program.[10] It also provided us with all the available supporting documentation it had for these agreements. For all the GA agreement documentation we reviewed, we found that none of the GA agreements addressed IT security. However, during our survey, we were informed that FSA was in the process of establishing and incorporating IT security in all future GA agreements to ensure compliance with Federal requirements and guidance. By including security language based on Federal requirements in GA agreements, FSA can increase its assurance that the necessary security controls are in place to protect information processed on behalf of the Department.

Including Federal security language in all contracts providing IT support or services, as well as all agreements for GAs, will help to ensure that system data, including PII, are protected from unauthorized access, use, disclosure, modification, or destruction. Including the security language also will allow for increased oversight of vendors, thus protecting FSA and the Department if security breaches occur from a vendor's system.

Suggested FSA Management Actions

We suggest that the Chief Operating Officer for FSA:

1. Ensure all contract documentation that specifies the name of the system for which the work is to be performed is accounted for in a centralized location such as the contract file and is timely provided when requested.

FSA Response

FSA management stated that during the survey, the survey team might have had difficulty in determining whether the contracts they were reviewing were for systems services or program services. They further stated that all of the contracts for system services had the names of the systems included in the contracts, and that corrective action is not required.

[10] The agreements it provided were primarily basic program agreements made under 34 C.F.R. § 682.401 although some of the agreements included additional provisions. However, from our review, not all documentation was included with each agreement. For example, for some of the agreements, we noted the attachments cited were missing.

OIG Response

The survey team worked with FSA staff to identify which contracts were for system services. Once FSA identified these contracts, we requested all documentation for each of the contracts. We were provided the hardcopy documentation for each of the contract files. Our review showed that for some of the contracts, names of the systems were not in the documentation we were provided. This condition was noted in the discussion draft that was provided to FSA management on June 27, 2011. During the exit briefing on June 30, 2011, FSA management did not indicate that documentation showing system names for the questioned contracts was available. On July 13, 2011, we issued our draft report. In its management response on August 4, 2011, FSA management stated that system names were included in all contracts for system services. However, it still did not provide the supporting documentation. Therefore, if this documentation existed outside of the contract files we reviewed, it needs to be accounted for in a centralized location. In our draft report, this management action originally suggested that FSA ensure that contracts specify the name of the system for which the work is to be performed. We have revised Suggestion 1. to address this issue.

2. Ensure that all contract documentation showing provisions to address IT security is accounted for in a centralized location such as the contract file and is timely provided when requested.

FSA Response

FSA management stated that after the release of the draft Management Information Report, all of FSA's current contracts contain IT security requirements and requested that this finding and Suggestion 2. be removed.

OIG Response

On January 21, 2011, when we first identified the seven contracts that did not contain documentation showing provisions to address IT security, while we were on site, we contacted our FSA point of contact to verify whether any documentation was missing. We did not receive any documentation. This condition was noted in the discussion draft that was provided to FSA management on June 27, 2011. On June 28, 2011, FSA personnel contacted OIG to request the information for the seven contracts. During the exit briefing on June 30, 2011, FSA management did not indicate that documentation showing provisions addressing IT security was available for the seven questioned contracts. On July 13, 2011, we issued our draft report. On July 15, 2011, FSA provided OIG documentation of provisions addressing IT security for the seven contracts. This documentation was not included in the contract files we reviewed and should have been accounted for in a centralized location. In our draft report, this management action originally suggested that FSA modify current contracts to appropriately address IT security and ensure that future contracts address IT security. We have revised Suggestion 2. to address this issue.

3. Ensure that all required C&A documentation can be readily located for the systems identified in the contract for which work is to be performed.

FSA Response

FSA stated that after the draft report was issued, it located the documents in OVMS and Outlook public folders. FSA is currently taking steps to store all of the records in OVMS and it expects to complete this project by the fall of 2011.

OIG Response

The survey team worked with FSA staff to locate C&A documents. However, by the end of survey, we still could not locate nor were we provided with the missing documents. After the issuance of the discussion draft, FSA requested and was provided an inventory of the missing C&A documents. During the exit briefing, the existence of these documents in OVMS and Outlook public folders was still not brought to our attention by FSA management. After the issuance of the draft report, FSA worked with the survey team to locate these documents. For C&A documents in Outlook public folders, we noticed that a user needed to access many different levels/folders to locate the documentation. Also, if a user did not know the exact folders users needed to access, the C&A documents could not easily be located. In addition, we noticed that for some C&A documents, there was not a standard naming convention that could easily identify the content of the document, further complicating our search for specific documentation. FSA's action to migrate documents housed in the Outlook public folders into OVMS will make these documents easier to locate. In our draft report, this management action originally suggested that FSA ensure that all required C&A documentation exists for the systems identified in the contract for which work is to be performed. We have revised Suggestion 3. to address this issue.

4. Create a centralized repository for all C&A information. This will ensure that all applicable C&A documentation is complete and can be readily located.

FSA Response

FSA management stated that it had implemented a centralized repository for all system related security documentation approximately 6 years ago in Outlook public folders for each system in FSA. OVMS had become FSA's central repository when it was able to capture C&A information in OVMS. FSA is currently moving the Outlook documents into OVMS and expects this transition to be completed by October 2011.

OIG Response

During our review, we found that C&A documentation was maintained in both the Outlook public folders and OVMS and not in a central repository. We found that documentation could not be readily located and we had to search both systems to locate a document. As cited in the suggested management action above, when using the Outlook public folders, the survey team encountered difficulty in locating C&A documentation. Centralizing C&A documentation into one repository will ensure that complete and up-to-date documentation can be readily located. We agree with FSA's corrective action to address this issue.

5. Ensure that existing and future GA agreements account for IT security.

FSA Response

FSA management stated that it will modify each guaranty agency's agreement to include a provision that addresses IT security to ensure that system data maintained by each agency, including PII, are protected.

OIG Response

Although we agree with FSA's corrective action to address this issue, a completion date for this action is needed.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of our survey was to first identify all FSA contracts providing contractor IT support or services to FSA or the Department, as well as all agreements for GA, which process, store, or transmit Department data through external IT systems as of November 1, 2010. Then, for each FSA contract identified, we determined whether the current contract contained any language that addressed IT security and whether documentation existed to support the C&A of the contractor's system. For each GA agreement identified, we determined whether the current agreement contained any language that addressed IT security. To satisfy this objective, we:

- reviewed applicable Federal requirements and guidance and Departmental policies and procedures;
- reviewed related Office of Inspector General (OIG) management information and audit reports and special projects;[11]
- reviewed the FY 2009 FISMA Annual Report relating to interconnection agreements, privacy impact assessments, and IT system certification and accreditation;
- reviewed the FY 2010 FISMA Annual Report relating to IT system certification and accreditation;
- conducted interviews with FSA management and staff responsible for managing FSA contracts and guaranty agreements; and
- evaluated relevant contracts, GA agreements, and supporting documentation to assess whether contracts and GA agreements appropriately address IT security.

Additional information on the scope and methodology is presented below.

Contract Review

We met with FSA contracting officials to identify all current contracts that provide some level of IT support to include processing, storing, or transmitting data on behalf of FSA or the Department. We received an initial list of 241 active FSA contracts. We reviewed all documentation for all 52 contracts that were related to contractor-provided IT support or services but focused on the Statements of Work (SOW)/Statements of Objectives (SOO) to determine which contracts were relevant to our objectives. After reviewing the SOW/SOOs for each contract file, we determined that 38 of those contracts met our objectives based on the NIST

[11] "Federal Student Aid's Efforts to Ensure the Effective Processing of Student Loans Under the Direct Loan Program," ED-OIG-X19K0008 (Management Information Report), dated September 16, 2010; "System Application Controls over the Financial Management System," ED-OIG-A11J0005 (Audit Report), dated September 2010; "Security over Certification and Accreditation for Information Systems," ED-OIG-A11J0001 (Audit Report), dated October 13, 2009; "Incident Handling and Privacy Act Controls over External Web Sites," ED-OIG-A11I006 (Audit Report), dated June 10, 2009; 2009 FISMA Annual Report, ED-OIG-S11J0008 (Special Project), dated November 17, 2009 and 2010 FISMA Annual Report, ED-OIG-S11K0002 (Special Project), dated November 12, 2010.

guidance identified in the background section. We also met with FSA contracting officials to discuss the documentation that supported the C&A process. For each contract file, we determined whether a SSP, SAR, and POA&M existed for each contractor system.

GA Agreements Review

We met with FSA contracting officials to identify all GA agreements that existed between FSA and the GAs. FSA also provided the supporting documentation for the GA agreements. We reviewed the agreements and all supporting documentation to determine whether IT security language was included in the GA agreements.

Our fieldwork was conducted from November 2010 through March 2011 at FSA contract offices located in Washington, D.C. An exit conference with FSA contract officials was held on June 30, 2011. We conducted our work in accordance with the OIG quality standards for Management Information Reports.

If you have any questions, please call Joseph Maranto, Director, Information Technology Audit Division, at 202-245-7044.

cc: Richard Gordon, Chief Information Officer, Federal Student Aid
Jay Hurt, Chief Financial Officer, Federal Student Aid
Bucky Methfessel, Senior Counsel for Information Technology, Office of General Counsel
Marge White, Audit Liaison for FSA

Attachment

Attachment

Abbreviations/Acronyms/Short Forms Used in this Report

C&A	Certification and Accreditation
C.F.R.	Code of Federal Regulations
Department	U.S. Department of Education
FFEL	Federal Family Education Loan
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
FSA	Federal Student Aid
GA	Guaranty Agency
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OVMS	Operational Vulnerability Management System
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
SAR	Security Assessment Report
SOO	Statements of Objectives
SOW	Statement of Work
SP	Special Publications
SSP	System Security Plan