**UNITED STATES DEPARTMENT OF EDUCATION**
OFFICE OF INSPECTOR GENERAL

INFORMATION TECHNOLOGY AUDIT DIVISION

September 22, 2014

**FINAL MANAGEMENT INFORMATION REPORT**

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

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

Subject: Review of Federal Student Aid's Oversight and Monitoring of Private Collection Agency and Guaranty Agency Security Controls
Audit Control Number **ED-OIG/X11N0003**

The purpose of this final management information report is to inform Federal Student Aid (FSA) of our concerns about its oversight and monitoring of private collection agency (PCA) and guaranty agency (GA) information security controls and make recommendations for addressing those concerns. The objective of our review was to gain a better understanding of how effective FSA's oversight and monitoring of PCA and GA operational controls were relating to the security of the U.S. Department of Education's (Department) information. We concluded that FSA did not provide adequate oversight of PCA and GA information security controls. Specifically, we found that (1) FSA did not issue a valid authorization to operate to any of the PCAs for an average of 8 months per PCA, (2) findings of security control deficiencies were not resolved timely, (3) FSA neither collected nor validated PCA training certificates as required, and (4) FSA has inadequate assurance that GA information system security complies with requirements of the Federal Information Security Management Act of 2002 (FISMA).

## BACKGROUND

The Department has contracted with PCAs to collect defaulted Federal student loans since 1981. Borrowers in default include students and parents. For our review period, the contractual relationship between the Department and the PCAs was governed by the 2009 PCA Task Order Award for Debt Collection and Administrative Resolution Services (task order). The Department awarded 5-year task orders to 23 PCAs in 2009 and currently contracts with

22 PCAs. The task orders were supplemented with statement of work requirements, which provided detailed information on contract deliverables, performance requirements, and computer system requirements. The computer system requirements in the task orders mandated that PCAs store Department student loan account records on their own computer systems, that access to Department account data was exclusively for default collection and resolution activities, and that PCAs provide the Department with the ability to remotely access PCA computer systems that store Department account records. PCAs and FSA share information on Department accounts through U.S. mail, telephone calls, a secure borrower Web site, secure email, and secure data transfers, which occur directly between PCA systems and FSA platforms over a "virtual private network" connection. The interconnection between PCA systems and the FSA platform requirements are covered by the Department's contract with PCAs and related agreements.

A GA is a State or private nonprofit agency that has agreements with the Secretary of Education to administer certain aspects of the Federal Family Education Loan (FFEL) Program, including insuring private lenders against losses due to a borrower's default.[1] Although there are no new FFEL Program loans because of a change in the Higher Education Act, which resulted in all new loans coming directly from the Department, GAs continue to insure FFEL Program loans already disbursed, perform default aversion activities, oversee lenders, collect defaulted FFEL Program loans, pay lender default claims, and report on loan statuses. Currently, 30 GAs participate in the FFEL Program.

GAs connect to the National Student Loan Data System, which is the central database for Title IV student financial aid and stores information about loans, grants, borrowers, lenders, GAs, schools, and servicers. At least monthly, GAs provide loan data to the Department on FFEL Program loans from loan origination until the loan is paid in full or closed for another reason. GAs receive data such as loan balances from lenders, which GAs then report to the Department. GAs also receive data, such as student enrollment status, from the Department; GAs need this data to service loans.

FISMA establishes a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, including operations and assets managed by another agency, contractor, or other source, such as PCAs and GAs. FISMA requires the Department to:

- assess the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- determine the levels of information security appropriate to protect information and information systems;
- implement policies and procedures to cost-effectively reduce risks to an acceptable level; and

[1] See 34 C.F.R. § 682.200 for FFEL Program details.

- periodically test and evaluate information security controls and techniques to ensure that they are effectively implemented.

FISMA established the National Institute of Standards and Technology (NIST) as the authority for establishing standards and guidance for Federal information system management.[2] NIST Special Publication 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems," states that contracts or other formal agreements for external providers handling Federal information or operating information systems on behalf of the Federal government must include security requirements. It also requires that mandated security authorization packages contain a security plan, a security assessment report, and a plan of action and milestones. FSA contracts with certification agents to assess each PCA's security plan and the security of the PCA's information systems. The certification agents create a security assessment report for each PCA. That report identifies the nature and severity of any security control weaknesses or deficiencies discovered in the information system and its operational environment and recommends related corrective actions and a plan of action and milestones.

The authorizing official for FSA systems, FSA's Chief Information Officer, uses the information from the certification agents to make risk-based authorization decisions. After reviewing the security authorization package and any additional information the certification agents provided, if the authorizing official determines that the risk to organizational operations and assets, individuals, and other organizations is acceptable, the authorizing official can issue an authorization to operate for the information system. The information system is authorized to operate for a specified time period in accordance with the terms and conditions the authorizing official established. The authorizing official also determines whether significant changes in the information systems or environments of operation require reauthorization. The authorizing official can deny authorization to operate an information system, or if the system is operational, halt operations if unacceptable risks exist.

FSA is responsible for ensuring that PCAs comply with information security requirements by conducting periodic site visits. FSA also oversees GAs to ensure that GAs adequately safeguard Department programs and information. PCAs and GAs collect and maintain sensitive financial and personally identifiable information (PII) pertaining to borrowers. Given the sensitive information and PII that PCA and GA systems process, FSA's assurance of the integrity of PCA and GA information technology systems is especially important.

## FINDINGS

We determined that FSA is not effectively overseeing and monitoring PCA and GA information security controls. We noted that (1) FSA did not issue a valid authorization to operate to any of the PCAs for an average of 8 months per PCA, (2) findings of security control deficiencies were not resolved timely, (3) FSA neither collected nor validated PCA training certificates as

[2] Enacted as Title III of the E-Government Act (Public Law 107-347), December 2002.

required, and (4) FSA has inadequate assurance that GA information system security complies with FISMA requirements.

**Finding 1. PCAs Operated Without Valid Authorizations to Operate**

During the time of our review, all 22 PCA contracts included a requirement that the PCAs undergo security authorization and obtain a valid authorization to operate from FSA's Chief Information Officer. The PCAs were granted authorization to operate on a 3-year basis and were required to obtain reauthorization every 3 years thereafter before the authorization expired. NIST Special Publication 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," now superseded, stated that Federal information systems should be reauthorized at least every 3 years or sooner if the system undergoes a significant change.[3] The reauthorization process was guided by NIST Special Publication 800-37, Revision 1, which required agencies to make timely risk management authorization decisions and have a risk determination process that provided a sufficient amount of time for reauthorizing systems within the 3-year requirement. An organization does not have to reauthorize a system if the organization has implemented information security continuous monitoring. According to the Chief Information Security Officer, the Department has not implemented information security continuous monitoring for PCA systems.

We found that for all 22 PCAs, FSA did not adequately process PCA system reauthorizations before their 3-year expiration. PCAs operated without a valid authorization to operate for a range of 85 to 375 days, or an average of 8 months per PCA. FSA improperly issued interim authorizations to operate for all 22 PCAs relying on OCIO-05, "Handbook for Information Technology Security Certification and Accreditation Procedures," March 2006, which states that the Department can issue interim authorizations to operate under certain conditions. However, the Department has not updated OCIO-05 to reflect the fact that the Office of Management and Budget has not recognized interim authorizations to operate as valid since fiscal year 2006.[4]

Without a valid authorization to operate, the Department has no assurance that the PCAs' systems had effective security controls, which means that they could have been vulnerable to attack. This, in turn, made the Department's systems vulnerable because of the interaction between the PCA's systems and the Department's. An attack on the PCAs' systems, which contain financial information and PII, could lead to unauthorized release and misuse of Federal student loan participant data, and reduced reliability and integrity of PCA and Department systems.

[3] NIST Special Publication 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," was superseded by Revision 4, in April 2013, which reflects new requirements for continuous monitoring in lieu of periodic authorizations. However, according to Office of Management and Budget Memorandum M-14-03, "Enhancing the Security of Federal Information and Information Systems," agencies are not required to implement continuous monitoring until 2017.

[4] See Office of Management and Budget Memorandum M-06-20, "Fiscal Year 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," July 2006.

**Finding 2. FSA Did Not Ensure that PCAs Timely Resolved Deficiencies**

FSA did not ensure that PCAs timely corrected information system deficiencies that certification agents identified during system reviews. Certification agents document these system deficiencies in the security assessment reports, which they upload in the Operational Vulnerability Management Solution. NIST Special Publication 800-53, Revision 3, "Recommended Security and Privacy Controls for Federal Information Systems and Organizations," required agencies to develop plans of action and milestones to document the organization's planned remedial actions and to reduce or eliminate known vulnerabilities in the system.[5] They also have to provide a completion date for their corrective actions. In addition, the Department's "Management of Plan of Action and Milestones Standard Operating Procedures" state that when the Department identifies findings for a given system, a plan of action and milestones is created that must be tracked and reported through closure of the corrective action. According to FSA's Chief Information Security Officer, FSA monitors the Operational Vulnerability Management Solution every 2 weeks to ensure PCAs have successfully performed corrective actions to resolve the deficiency. Furthermore, PCAs must resolve all deficiencies before FSA grants authorizations to operate. If a PCA does not resolve a deficiency, FSA has the authority to disconnect the PCA from its internal platform.

Analyzing data from the Operational Vulnerability Management Solution, we found that as of December 2013, the 22 PCAs had 833 deficiencies being tracked in Operational Vulnerability Management Solution. Of those 833 deficiencies, 820 were classified as resolved. However, we found that 778 were resolved after the estimated completion date, an average of 71 days (between 1 and 301 days) late. The 13 deficiencies that remained open as of December 2013 had not been resolved for an average of 171 days (between 154 and 216 days) after the estimated completion date, with no apparent repercussions for the PCAs. A majority of the open deficiencies pertained to PCAs not implementing two-factor authentication for network and logical access to its systems.

Because PCA systems communicate not only with internal FSA platforms, but also with borrowers, other loan servicers, third-party data providers, consumer reporting agencies, guarantors, and other government agencies, the PCAs have an increased risk that their information systems may be compromised, resulting in a risk to organizational operations, assets, individuals, and other organizations.

[5] Although NIST Special Publication 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," was superseded, the requirement for plans of action and milestones was carried over into NIST Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations."

**Finding 3. FSA Did Not Ensure That PCAs Complied With Training Requirements**

FSA did not ensure that PCAs complied with training requirements. As part of its PCA site visits, FSA monitors are responsible for verifying that PCA employees and subcontractors completed the mandatory annual security awareness training required by the contracts between the PCAs and the Department.

The Department's PCA Procedures Manual states that before PCA begin any collection activity on Department accounts, all of its employees and subcontractors, must annually receive training and provide signed certifications that they received required training regardless of whether or not they have provided certifications on past Department contracts. The manual further clarifies that PCAs must not only maintain signed certifications on file, but also forward them to FSA's Processing Division in Atlanta Regional Office, which oversees PCA training, within 5 calendar days after completion of training. PCAs must also annually submit to FSA reports on security awareness and Privacy Act training.

According to the FSA Information System Security Officer, during the site visits, FSA neither requested nor verified the required documentation of mandatory training. FSA also did not determine whether the PCAs had sent the required documentation to FSA's Atlanta office nor maintained that documentation as required. In addition, FSA could not provide evidence that all employees received the mandatory training. Rather, FSA relied on incomplete PCA-generated training rosters without verifying or cross-referencing them with actual training certificates. The training rosters that FSA provided to us for review lacked required information, making it impossible to accurately account for the training or to validate that PCA employees met the training requirements.

Without adequate oversight of training documentation, the Department has no assurance that PCAs provided their employees and subcontractors with all the required training necessary to carry out their responsibilities in compliance with information security requirements that are necessary to protect Department systems and data.

**Finding 4. FSA Has Inadequate Assurance that GA Information System Security Complies with FISMA Requirements**

We found that all 30 current GA agreements lacked provisions for system security requirements that would have permitted FSA to meet its obligations to ensure that data supporting Department operations is adequately safeguarded as required by FISMA. GA operations are governed by agreements between the Department and individual GAs.[6] The current GA agreements do not

[6] Because GAs connect to the National Student Loan Data System, they are also governed by the National Student Loan Data System Security Plan and the Department's Data Provider Instructions. The System Security Plan for National Student Loan Data System provides an overview of the security requirements of the system and describes the controls in place or planned for meeting those requirements, as well as delineates responsibilities and expected behavior of all individuals who access the system. The Department's Data Provider Instructions assist users with the data provider portion of the National Student Loan Data System update process and provides basic information about the entire process.

contain any information technology security requirements, nor do they require FSA to oversee GAs to ensure GAs are complying with FISMA. We previously noted this deficiency in our September 2011 management information report on FSA contracts and GA agreements (ED-OIG/X11L0002). FSA stated in response to the report that it would modify each GA agreement to include a provision that addresses information technology security to ensure that system data the GA maintains, including PII, are protected. As of February 2014, none of the agreements included such a provision.

In addition, FSA's oversight of GA information technology security controls is limited to unofficial reviews with no required corrective actions by GAs when FSA identifies deficiencies. Before an on-site visit to a GA, the FSA Technology Office requires the GA to complete a self-assessment questionnaire and checklist that does not ask questions about any specific risk areas, but rather asks only generic questions, such as, "Do you have a privacy program that includes policies, controls, training, and an incident response plan (including cyber events)?"[7] An FSA technical team reviews the GA's completed self-assessment checklist and also reviews the GA's policies and procedures related to privacy, security and other relevant documents, such as system security plans and previous audit reports. During onsite reviews, the FSA technical team interviews senior GA leadership and key stakeholders in operations and security, with a focus on verifying and clarifying GA self-assessment answers and questions raised by the previsit document reviews. FSA then uses the GA's self-assessment checklist to perform a high-level evaluation of certain operational controls related to the GA's data security environment, with a specific focus on protection of PII, resulting in what FSA refers to as a security assessment report. Because FSA does not require GAs to take any corrective actions, none of the deficiencies that FSA identifies in the report are tracked in the Operational Vulnerability Management Solution. Because these security assessment reports do not address specific risk areas and do not require corrective actions, the reports do not evaluate GA information security consistent with the requirements of FISMA and NIST Special Publication 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems."

Because FSA does not have sufficient assurance regarding the information system security of GAs, it is not meeting its obligation to ensure the integrity of system data, including PII, and the protection of the data from unauthorized access, misuse, disclosure, and destruction.

**Recommendations**

We recommend that the FSA Chief Operating Officer:

1. Ensure that PCAs systems are reauthorized every 3 years, or as appropriate under new continuous monitoring requirements.

[7] The self-assessment checklist was introduced at the GA Security and Privacy Conference in June 2010 in response to a security breach. The intent of the self-assessment checklist is to evaluate individual GA system security controls identified in NIST Special Publication 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations."

2. Disallow PCA interaction with FSA internal platforms until they have valid authorizations to operate.
3. Discontinue the use of interim authorizations to operate for PCAs and update OCIO-05, "Handbook for Information Technology Security Certification and Accreditation Procedures," to reflect current requirements.
4. Ensure each PCAs meet training requirements and verify their certificates of completion.
5. Ensure that PCAs timely perform corrective actions to resolve system weaknesses and deficiencies.
6. Either amend current GA agreements to include appropriate information technology security requirements, or pursue other alternatives to ensure protection of GA information systems that support Department programs.
7. Ensure that FSA sufficiently oversees GA information technology security to satisfy security requirements under FISMA, and
8. Ensure for all future engagements that FSA provides the OIG audit team with the most current complete and accurate documentation.

**FSA Response**

OIG provided a draft of this management information report to FSA for comment on June 17, 2014. In its response, dated July 17, 2014, FSA stated that it appreciated our concerns and recognized the importance of monitoring information security controls. Although FSA officially concurred with recommendations 1, 2, 3, 4, 5, and 7, it offered further clarifications to recommendation 1, 2, 6, and 7.

For recommendation 1, FSA stated that it had inadvertently placed authorizations to operate for PCAs in an outdated folder, resulting in the review of inaccurate information. As a result, it provided further documentation to the OIG on February 28, 2014 and again on July 9, 2014. FSA also stated that it did issue authorizations to operate for less than three years (short-term authorizations to operate) to PCAs under the condition that the information system owner continue to make progress in correcting identified security control deficiencies for the system. According to FSA, the short-term authorizations to operate served an additional purpose and specifically enhanced monitoring and tracking of the plan of action and milestones associated with each of the control deficiencies by not only the information system owner, but also the Information System Security Officer and FSA Technology office staff.

For recommendation 2, FSA confirmed that it had a few existing PCA systems for which a previous ATO expired before FSA completed a new ATO. As result, it will decide whether to terminate PCA interaction with FSA internal platforms based on the risk, security posture, the status of the PCA system in the ATO process, and the nature of security deficiencies, in accordance to NIST SP 800-37, Revision 1, Risk Management Framework.

For recommendation 6, FSA did not provide any specific actions to address our recommendation nor did it provide a date by which any actions would be completed. Rather, it provided a general statement stating that through a collaborative engagement with appropriate offices within FSA

and the Department, FSA will investigate flexibilities that may exist with respect to the existing GA agreements and will exercise such flexibilities as determined to be appropriate.

For recommendation 7, FSA did not provide any specific actions to address our recommendation nor did it provide a date by which any actions would be completed. Rather, it stated that it will investigate the use of GA internal audits to assess compliance with FISMA requirements, in consultation with OIG and other Department offices.

We included FSA's response in its entirety as Attachment B to this report.

**OIG Comments**

We reviewed FSA's response and comments to recommendations 3, 4, and 5, and found them to be responsive to our recommendations. We also reviewed FSA's additional clarifications pertaining to recommendations 1, 2, 6, and 7, but found them to be inadequate and unresponsive. With regard to recommendation 1, FSA attributed the lapse of time between the authorizations to operate to it placing documentation in an outdated folder that resulted in reviewing inaccurate information. FSA also stated that under certain conditions, it relied on what it describes as "short-term authorizations to operate." Throughout fieldwork, OIG provided FSA with multiple opportunities to supply current and accurate supporting documents. Each time FSA provided additional support for the authorizations to operate, it assured OIG that all current and accurate documents were furnished. The documents that FSA recently provided us on July 9, 2014, after we provided FSA the draft report, were both duplicate copies of what FSA originally submitted to us and new documents that FSA never previously provided us. Furthermore, what FSA calls "short-term ATOs" that enhance monitoring and tracking, are interim authorizations that are not permitted, as OMB only allows for three-year authorizations to operate or continuous monitoring. FSA cannot use a different terminology for the same process and expect it to be allowable.

FSA's submission of duplicate and new documents caused OIG staff to expend unnecessary time and effort and did not result in any clarification or modifications to the evidence the OIG collected during the fieldwork or in any changes to our findings or recommendations. FSA providing inaccurate initial information and providing new documents after OIG fieldwork is complete has occurred in past audits of FSA. For example, during the time for management response and long past completion of OIG fieldwork for the FY12 FISMA audit, FSA informed us that it provided the wrong supporting documents. After that, FSA committed to us that on all future engagements, FSA management would personally approve all documents provided to the auditors to ensure the provision of current correct and complete documents every time.

Despite FSA's commitment to provide current correct and complete documents, FSA continues to provide us with what it should know are not the documents we have requested. Not ensuring that it provides current, correct, and complete documents to the OIG forces our office to expend unnecessary resources to review irrelevant, duplicate, and incorrect information, and causes unnecessarily delays to the audit. To ensure that FSA establishes an effective process for providing documents to auditors, we added recommendation 8.

FSA's response to recommendation 2 did not adequately address our recommendation. Despite our recommending that FSA disallow PCA interaction with FSA internal platforms pending valid authorizations to operate, FSA indicated that it will decide whether to terminate PCA interaction with FSA internal platforms based on risk, and other NIST-recommended factors. In addition, FSA did not specify how it plans to accomplish this nor did it provide a date by which any corrective actions would be completed. Therefore, we found FSA's proposed corrective action to be unresponsive.

FSA's response to recommendation 6 did not adequately address our recommendation. Rather, FSA indicated that it will look into this matter and, with cooperation of appropriate offices and the Department, investigate flexibilities that may exist with respect to the existing GA agreements. Although OIG recommended specific actions, including FSA pursuing alternatives to amending the GA agreements, FSA's response did not identify what actions it would take to ensure protection of GA information systems that support Department programs. Therefore, we found FSA's proposed corrective action to be unresponsive.

FSA's response to recommendation 7, although a step in the right direction, did not include any specific corrective action. Rather, FSA stated that it will investigate the use of GA internal audits to assess compliance with FISMA requirements, in consultation with OIG and other Department offices. It did not provide any details on its plan to oversee GAs' information technology security to satisfy security requirements under FISMA. Therefore, we found FSA's proposed corrective action to be unresponsive.

Based on FSA's response, OIG agrees with FSA's proposed corrective actions to recommendations 3, 4, and 5, but does not agree with its proposed corrective actions for recommendations 1, 2, 6, and 7. In addition, to highlight the importance of FSA providing the OIG with current correct and complete documents, OIG added recommendation 8.

## OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of our review was to gain a better understanding of how effective FSA's oversight and monitoring of PCA and GA operational controls are relating to the security of the Department's information. To satisfy this objective, we performed the following:

- obtained an understanding of FSA's oversight and monitoring process for PCA and GA security controls, from the Department's Technology Office and Business Operations Security Division;
- reviewed applicable Federal requirements, guidance, and Departmental policies and procedures;
- examined Department's training requirements for Federal employees and compared it with PCAs to ensure PCA compliance with these requirements;

- used the Operational Vulnerability Management Solution database to determine the number of information security deficiencies that had been identified for the PCAs and to determine the plan of action and milestones for each deficiency;
- reviewed and analyzed individual PCA contracts dated July 2009, awarded for a period of 5 years;
- reviewed PCA information technology system security certifications and authorizations to operate;
- reviewed and evaluated current GA agreements with the Department, the National Student Loan Data System Security Plan, the Department's Data Provider Instructions, and other supporting documentation to assess whether GA agreements appropriately addressed information technology security; and
- interviewed key FSA management and staff responsible for oversight and monitoring of PCAs and GAs. From the Technology Office and Business Operations Security Division, we interviewed the Chief Information Security Officer, Director of Business Operations Security Division, PCA Manager, Information Systems Security Officer, and Chief Risk Officer.

In addition, we reviewed prior management information reports, final alert memorandums, audit reports, and other key documents specifically relating to PCAs and GAs issued by Department, the Department of the Treasury, and the United States Government Accountability Office. These reports included:

- "Survey of Federal Student Aid Contracts and GA Agreements," September 2011 (ED-OIG/X11L0002);
- "Federal Student Aid Paid Private Collection Agencies Based on Estimates," May 2013 (ED-OIG/L02N0002);
- "Privacy Impact Assessment of PCAs," September 2012;
- "Verbal Complaints Against Private Collection Agencies," May 2013 (ED-OIG/L06M0012);
- "Audit of the Department's Compliance with the Federal Information Security Management Act," October 2011 (ED-OIG/A11L0003);
- "Review for New Hampshire Higher Education Assistance Foundation," October 2012;
- "U.S. Department of Education, FY 2013 Management Challenges," January 2013;
- "U.S. Department of Education, FY 2012 Management Challenges," October 2011;
- "FEDERAL STUDENT LOAN PROGRAMS: Opportunities Exist to Improve Audit Requirements and Oversight Procedures," July 2010 (GAO-10-668);
- "U.S. Department of Education OIG Semiannual Report to Congress, No. 67," December 2013;
- "GOVERNMENT-WIDE FINANCIAL MANAGEMENT: The Financial Management Service Implemented Corrective Actions for Private Collection Agencies," September 2012 (OIG-12-071); and
- "U.S. Department of Education FY 2012 Agency Financial Report—Other Accompanying Information," November 2012.

We conducted a site visit at FSA to identify current GA agreements that existed between FSA and the GAs. We reviewed the agreements and all supporting documentation to determine whether information technology security language related to FISMA requirements was included in any of these agreements.

Our fieldwork was conducted from October 2013 through January 2014. We held an exit conference with FSA on February 26, 2014. We conducted our work in accordance with the Council of the Inspectors General on Integrity and Efficiency "Quality Standards for Inspection and Evaluation."

## ADMINISTRATIVE MATTERS

This management information report issued by the Office of Inspector General will be made available to members of the press and general public to the extent information contained in the report is not subject to exemptions in the Freedom of Information Act (5 U.S.C. § 552) or protection under the Privacy Act (5 U.S.C. § 552a).

We appreciate the cooperation given to us during this review. If you have any questions, please call Joseph Maranto at (202) 245-7044.

cc: Jerry E. Williams, Chief Information Officer, Federal Student Aid
Linda Wilbanks, PhD, Chief Information Security Office, Federal Student Aid
Bucky Methfessel, Senior Counsel for Information Technology, Office of General Counsel
Dawn Dawson, Audit Liaison for Federal Student Aid

Attachments

**Attachment A**

## Abbreviations/Acronyms/Short Forms Used in this Report

| | |
|---|---|
| Department | U.S. Department of Education |
| FFEL | Federal Family Education Loan |
| FISMA | Federal Information Security Management Act of 2002 |
| FSA | Federal Student Aid |
| GA | Guaranty Agency |
| NIST | National Institute of Standards and Technology |
| PCA | Private Collection Agency |
| PII | Personally Identifiable Information |
| Task Order | 2009 PCA Task Order Award for Debt Collection and Administrative Resolution Services |

**Attachment B**

July 17, 2014

To: Charles E. Coe, Jr.
Assistant Inspector General for
Information Technology Audits and Computer Crime Investigations
Office of Inspector General

From: James W. Runcie
Chief Operating Officer
Federal Student Aid

Subject: Draft Management Information Report: "Review of Federal Student Aid's Oversight and Monitoring of Private Collection Agency and Guaranty Agency Security Controls," Audit Control Number ED-OIG/X11N0003

Thank you for providing us with an opportunity to respond to the Office of Inspector General's (OIG) draft management information report regarding your concerns about Federal Student Aid's (FSA) oversight and monitoring of private collection agency (PCA) and guaranty agency (GA) information security controls.

FSA's management appreciates your concerns and recognizes the importance of monitoring information security controls. We have taken a number of steps to strengthen our oversight efforts, many of which predate this review, and directly respond to the seven recommendations included in your report to improve oversight and monitoring of PCA and GA operational controls.

Specifically, for example, over the past three years, FSA has moved all 17 systems supported by the FSA Virtual Data Center (VDC), including the VDC, under continuous monitoring through the ongoing authorization program and is in the planning stages to transition the external systems and partners, including the PCAs, into this program. FSA initiated bi-weekly scans utilizing the Qualys tool for vulnerability management, such as zero day vulnerabilities, patch management and version control; this is planned for the PCAs as part of moving them into the ongoing authorization program. FSA issued Authority to Operate (ATO) certificates for shorter than the three-year cycle when it was determined the security risks of the system required greater visibility for tracking those risks to closure.

**Attachment B**

Page 2

Our response to each of these recommendations follows:

**Recommendation 1: Ensure that PCAs systems are reauthorized every 3 years, or as appropriate under new continuous monitoring requirements.**

FSA concurs with this recommendation.

Finding 1 states (in part) that "PCAs operated without a valid authorization to operate for a range of 85 to 375 days, or an average of 8 months per PCA."

FSA's data indicates the following:

| # PCAs | ATO |
|---|---|
| 10 | On time |
| 10 | 1 day lapse |
| 1 | 2 lapses ( 4 & 12 days) |
| 1 | 2 lapses (18 & 30 days) |
| 1 | 1 lapse (90 days) |

In a review of the information provided for the audit, FSA discovered it had inadvertently placed the ATO documents in an outdated folder, resulting in the review of inaccurate information.

FSA did issue ATOs for less than three years (short term ATOs) to PCAs under the condition that the information system owner continue to make progress in correcting identified security control deficiencies for the system. The short-term ATOs served an additional purpose -- enhanced monitoring and tracking of the Plan of Action and Milestones (POA&Ms) associated with each of the control deficiencies by not only the information system owner, but also the Information System Security Officer (ISSO) and FSA Technology office staff.

FSA will take the following actions to implement the recommendation:

- FSA will implement procedures to validate information provided is current and accurate prior to submission.
- The historical ATO documents that reside in the Interim ATO folder will be moved to the ATO folder, and the Interim ATO folder will be deleted.

**Attachment B**

Page 3

- FSA will update the ATO process and procedures to adhere to the three year certification requirement.
- FSA will develop a plan to implement the three year ATO for all PCAs.
- To prevent a lapse in ATOs, the updated procedures will include establishing re-authorization timelines to be executed to facilitate sufficient time to complete the re-authorization process.

**Recommendation 2: Disallow PCA interaction with FSA internal platforms until they have valid authorizations to operate.**

FSA concurs with this recommendation.

However, FSA does not allow new PCA systems any data transfers until they have received a full ATO. We agree there have been a few existing PCA systems for which a previous ATO expired before FSA completed a new ATO for the system.

In addition to the actions identified in response to recommendation 1 above, when an ATO has expired, FSA will decide whether to terminate PCA interaction with FSA internal platforms. FSA's decision will be based on the risk of the situation after evaluating the security posture of the PCA system; the status of the PCA system in the ATO process; and the nature of security deficiencies that have been identified per National Institute of Standards and Technology (NIST) SP 800-37's, Revision1 Risk Management Framework.

**Recommendation 3: Discontinue the use of interim authorizations to operate for PCAs and update OCIO-05, "Handbook for Information Technology Security Certification and Accreditation Procedures," to reflect current requirements.**

FSA concurs with this recommendation.

FSA will support the Department in the updating of OCIO-05 "Handbook for Information Technology Security Certification and Accreditation Procedures." FSA will work with the Department to ensure the update reflects specific direction for compliance with appropriate NIST and Office of Management and Budget (OMB) directives that have been issued since the drafting of OCIO-05 and will adhere to the revised Handbook accordingly.

**Attachment B**

Page 4

**Recommendation 4: Ensure each PCA meets training requirements and verify their certificates of completion.**

FSA concurs with this recommendation.

FSA will revise its internal procedures used to verify PCA employee compliance with FSA's information security training requirements.

**Recommendation 5: Ensure that PCAs timely perform corrective actions to resolve system weaknesses and deficiencies.**

FSA concurs with this recommendation.

FSA will take the following actions to implement the recommendation:

- FSA will implement a more rigorous review of the corrective action due dates in each PCA's POA&Ms, to ensure that the PCA staff has both the time and the understanding of the security weaknesses and deficiencies to resolve them by applicable due dates.
- FSA will conduct additional in-depth reviews during weekly reviews of PCAs' POA&M status.
- FSA will engage PCAs' contracting officers and ISSOs to assist in timely closure of all actions.
- FSA will modify current monthly IT security meetings with the Department to include a review of the PCAs' status of corrective actions.

**Recommendation 6: Either amend current GA agreements to include appropriate information technology security requirements, or pursue other alternatives to ensure protection of GA information systems that support Department programs.**

Through a collaborative engagement with appropriate offices within FSA and the Department, FSA will investigate flexibilities that may exist with respect to the existing GA agreements and will exercise such flexibilities as determined to be appropriate.

**Recommendation 7: Ensure that FSA sufficiently oversees GA information technology security to satisfy security requirements under FISMA.**

**Attachment B**

Page 5

FSA concurs with this recommendation.

FSA will investigate the use of existing GA internal audits to assess compliance with Federal Information Security Management Act (FISMA) requirements, in consultation with OIG and other Department of Education offices.

Once again, thank you for allowing us to comment on the draft management information report.