



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

THE INSPECTOR GENERAL

November 14, 2014

The Honorable Arne Duncan
Secretary of Education
Washington, D.C. 20202

Dear Secretary Duncan:

The enclosed reports present the results of the audit of the U.S. Department of Education's (Department) financial statements for fiscal years 2014 and 2013 to comply with the Chief Financial Officers Act of 1990, as amended. The reports should be read in conjunction with the Department's financial statements and notes to fully understand the context of the information contained therein.

We contracted with the independent certified public accounting firm of CliftonLarsonAllen, LLP (CliftonLarsonAllen) to audit the financial statements of the Department as of September 30, 2014 and 2013, and for the years then ended. The contract requires that the audit be performed in accordance with U.S. generally accepted government auditing standards and Office of Management and Budget bulletin, *Audit Requirements for Federal Financial Statements*.

Results of the Independent Audit

CliftonLarsonAllen found:

- The fiscal years 2014 and 2013 financial statements are presented fairly, in all material respects, in accordance with accounting principles generally accepted in the United States of America;
- One significant deficiency in internal control over financial reporting; and
- One instance of reportable noncompliance with certain provisions of the Debt Collection Improvement Act of 1996, as amended.

Evaluation and Monitoring of Audit Performance

The Inspector General Act of 1978 requires that the Inspector General take appropriate steps to assure that any work performed by non-Federal auditors complies with the audit standards established by the Comptroller General. In that regard, we evaluated the independence, objectivity, and qualifications of the auditors and specialists; reviewed the plan and approach of the audit; monitored the performance of the audit; reviewed CliftonLarsonAllen's reports and related audit documentation; and inquired of its representatives.

400 MARYLAND AVENUE, S.W., WASHINGTON, DC 20202-1510

Promoting the efficiency, effectiveness, and integrity of the Department's programs and operations.

Page 2 – The Honorable Arne Duncan

Our review was not intended to enable us to express, and we do not express, an opinion on the Department’s financial statements, or conclusions about the effectiveness of internal control, whether the Department’s financial management systems substantially complied with the Federal Financial Management Improvement Act of 1996, or on compliance with laws and regulations.

CliftonLarsonAllen is responsible for the enclosed auditors’ report and the conclusions expressed in the related reports on internal control and compliance with laws and regulations. Our review disclosed no instances where CliftonLarsonAllen did not comply, in all material respects, with U.S. generally accepted government auditing standards.

We appreciate the cooperation given CliftonLarsonAllen and my office during the audit. If you have any questions or would like to discuss the reports, please contact me at (202) 245-6900.

Sincerely,



Kathleen S. Tighe
Inspector General

Enclosure



CliftonLarsonAllen LLP

www.cliftonlarsonallen.com

INDEPENDENT AUDITORS' REPORT

Inspector General
United States Department of Education

Secretary
United States Department of Education

Report on the Financial Statements

We have audited the accompanying financial statements of the United States Department of Education (Department), which comprise the consolidated balance sheets as of September 30, 2014 and 2013, and the related consolidated statements of net cost and changes in net position, and the combined statements of budgetary resources for the years then ended, and the related notes to the financial statements (financial statements).

Management's Responsibility for the Financial Statements

The Department's management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America (U.S.) and the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditors' Responsibility

Our responsibility is to express an opinion on these financial statements based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the U.S.; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 14-02, *Audit Requirements for Federal Financial Statements* (OMB Bulletin 14-02). Those standards and OMB Bulletin 14-02 require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditors' judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of

INDEPENDENT AUDITORS' REPORT (Continued)

significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

We are also responsible for applying certain limited procedures with respect to the Required Supplementary Information and Other Information included with the financial statements.

Opinion on the Financial Statements

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of the United States Department of Education as of September 30, 2014 and 2013, and its net costs, changes in net position, and budgetary resources for the years then ended, in accordance with accounting principles generally accepted in the U.S.

Other Matters

Required Supplementary Information

Accounting principles generally accepted in the U.S. issued by the Federal Accounting Standards Advisory Board (FASAB) require that the Department's Management Discussion and Analysis (MD&A), other Required Supplementary Information (RSI), and Required Supplementary Stewardship Information (RSSI) on pages 1 through 48 and 95 through 101 of the United States Department of Education's FY 2014 Agency Financial Report, be presented to supplement the financial statements. Such information, although not a part of the financial statements, is required by FASAB, who considers it to be an essential part of financial reporting for placing the financial statements in an appropriate operational, economic, or historical context. We have applied certain limited procedures to the MD&A, other RSI, and RSSI in accordance with auditing standards generally accepted in the U.S., which consisted of inquiries of management about the methods of preparing the information and comparing the information for consistency with management's responses to our inquiries, the financial statements, and other knowledge we obtained during our audit of the financial statements. We do not express an opinion or provide any assurance on this information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

Other Information

The Message from the Secretary, Message from the Chief Financial Officer, and the Other Information on pages iii and iv, 50 and 51, and 119 through 150, of the United States Department of Education's FY2014 Agency Financial Report, respectively, contain a wide range of information, some of which is not directly related to the financial statements. This information is presented for purposes of additional analysis and is not a required part of the financial statements or RSI. This information has not been subjected to the auditing procedures applied in the audit of the financial statements, and accordingly, we do not express an opinion or provide any assurance on it.

INDEPENDENT AUDITORS' REPORT (Continued)**Report on Internal Control over Financial Reporting and Report on Compliance Based on an Audit of Financial Statements Performed in Accordance with *Government Auditing Standards******Report on Internal Control over Financial Reporting***

In planning and performing our audit of the financial statements, we considered the Department's internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Department's internal control or on management's assertion on internal control included in the MD&A. Accordingly, we do not express an opinion on the effectiveness of the Department's internal control or on management's assertion on internal control included in the MD&A.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A *material weakness* is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the Department's financial statements will not be prevented, or detected and corrected on a timely basis. A *significant deficiency* is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control, described below and in more detail in Exhibit A, which we consider to be a significant deficiency.

Department and Federal Student Aid Management Need to Mitigate Persistent
Information Technology Control Deficiencies

Due to the unique requirements of the Department's grant, loan and administrative business activities, the Department manages its general support system and core financial management system and oversees a large portfolio of Federal Student Aid (FSA) or contractor owned information systems. The third party servicers who manage FSA's general support systems and contractor-owned and contractor operated financial systems are monitored by FSA management through the use of Service Level Agreements and third party independent reviews. We continued to identify control deficiencies in the areas of security management, personnel security, access controls, and configuration management across these systems. These deficiencies can increase the risk of unauthorized access to the Department's systems used to capture, process, and report financial transactions and balances, affecting the reliability and security of the data and information.

INDEPENDENT AUDITORS' REPORT (Continued)

Report on Compliance

As part of obtaining reasonable assurance about whether the Department's financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements consistent with our professional responsibilities discussed below.

The results of our tests, exclusive of those required by the Federal Financial Management Improvement Act of 1996 (FFMIA) as discussed below, disclosed one instance of noncompliance with respect to a certain aspect of the Department's debt collection activities, described in Exhibit B, that is required to be reported in accordance with *Government Auditing Standards* and OMB Bulletin No. 14-02.

Compliance with FFMIA Requirements

Under FFMIA, we are required to report whether the financial management systems used by the Department substantially comply with the FFMIA Section 803(a) requirements. To meet this requirement, we performed tests of compliance with (1) Federal financial management systems requirements, (2) applicable Federal accounting standards, and (3) the United States Standard General Ledger (USSGL) at the transaction level. However, providing an opinion on compliance with FFMIA was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests of FFMIA Section 803(a) requirements disclosed no instances in which the Department's financial management systems did not substantially comply with (1) Federal financial management systems requirements, (2) applicable Federal accounting standards, or (3) the USSGL at the transaction level.

Management's Responsibility for Internal Control and Compliance

Management is responsible for (1) evaluating the effectiveness of internal control over financial reporting based on criteria established under the Federal Managers' Financial Integrity Act (FMFIA), (2) providing a statement of assurance on the overall effectiveness on internal control over financial reporting, (3) ensuring the Department's financial management systems are in substantial compliance with FFMIA requirements, and (4) complying with other applicable laws, regulations, contracts, and grant agreements.

Auditors' Responsibilities

We are responsible for: (1) obtaining a sufficient understanding of internal control over financial reporting to plan the audit, (2) testing whether the Department's financial management systems substantially comply with the FFMIA requirements referred to above, and (3) testing compliance with certain provisions of laws, regulations, contracts and grant agreements that have a direct and material effect on the determination of the financial statement amounts and applicable laws and regulations for which OMB Bulletin 14-02 requires testing.

We did not evaluate all internal controls relevant to operating objectives as broadly established by the FMFIA, such as those controls relevant to preparing statistical reports and ensuring efficient operations. We limited our internal control testing to testing controls over financial reporting. Because of inherent limitations in internal control, misstatements due to error or fraud, losses or noncompliance may nevertheless occur and not be detected. We also caution that projecting our audit results to future periods is subject to risk that controls may become inadequate because of changes in conditions or that the degree of compliance with controls

INDEPENDENT AUDITORS' REPORT (Continued)

may deteriorate. In addition, we caution that our internal control testing may not be sufficient for other purposes.

We did not test compliance with all laws, regulations, contracts and grant agreements applicable to the Department. We limited our tests of compliance to certain provisions of laws, regulations, contracts and grant agreements that have a direct and material effect on the determination of financial statement amounts and applicable laws and regulations for which OMB Bulletin 14-02 requires testing. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. We caution that noncompliance may occur and not be detected by these tests and that such testing may not be sufficient for other purposes. Also, our work on FFMA would not necessarily disclose all instances of noncompliance with FFMA requirements.

Management's Response to Findings

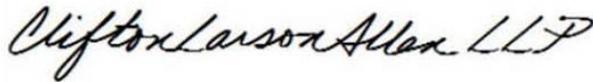
Management's response to the findings identified in our report is presented in Exhibit C. We did not audit the Department's response and, accordingly, we express no opinion on it.

Status of Prior Year's Control Deficiencies and Noncompliance Issues

We have reviewed the status of the Department's corrective actions with respect to the findings included in the prior year's Independent Auditors' Report, dated December 11, 2013. The status of prior year findings is presented in Exhibit D.

Purpose of the Report on Internal Control over Financial Reporting and the Report on Compliance

The purpose of the Report on Internal Control over Financial Reporting and the Report on Compliance sections of this report is solely to describe the scope of our testing of internal control and compliance and the result of that testing, and not to provide an opinion on the effectiveness of the Department's internal control or on compliance. These reports are an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the Department's internal control and compliance. Accordingly, these reports are not suitable for any other purpose.

**CliftonLarsonAllen LLP**

Arlington, Virginia
November 14, 2014

INDEPENDENT AUDITORS' REPORT (Continued)
EXHIBIT A
Significant Deficiency

Department and Federal Student Aid Management Need to Mitigate Persistent Information Technology Control Deficiencies

Due to the unique requirements of the Department's grant, loan and administrative business activities, the Department oversees a large portfolio of government owned and operated, government owned and contractor operated, and contractor owned and operated information systems. Four Federal Student Aid (FSA) systems and one Department system comprise the key financial systems. The third party servicers who manage the Department and FSA's general support systems and contractor owned and operated financial systems are monitored by the Department and FSA management through the use of Service Level Agreements and independent reviews. Managing the information and system security across the Department is the responsibility of the Department's Chief Information Security Officer (CISO), in conjunction with FSA's CISO. For several years, financial and other audits have identified numerous system deficiencies that affect the security and reliability of the information within these systems. Last year, we noted information technology (IT) control deficiencies in the areas of security management, personnel security, access controls, incident response, configuration management, and contingency planning in one or more systems. In addition, last year we noted application-level control issues for four of the seven independent reviews of FSA's contractor owned and operated systems. Based on testing performed this year, we noted no control deficiencies in the areas of incident response and contingency planning. During fiscal year (FY) 2014, FSA implemented an oversight function involving FSA's Business Operations and Finance offices to closely monitor completion of corrective action plans for the noted control deficiencies. This year, none of the independent reviews identified significant system control deficiencies. Despite these improvements, our audit continued to identify control deficiencies in the following areas:

Security management

- The Department's IT policies and procedures and certain system security plans were outdated or did not fully address specific controls required by the National Institute of Standards and Technology (NIST)
- Annual security control assessments were not completed
- Security assessments and authorization of certain systems did not comply with NIST requirements
- System risk assessments were not kept current
- System vulnerabilities were not being formally tracked through remediation
- Mitigation strategies for corrective actions related to IT control weaknesses were missing and corrective action deadlines were missed
- Security awareness training for new system users was not always completed
- Role based security awareness training for users with significant system security responsibilities was not always completed

Personnel security

- Background reinvestigations were not completed timely by the Department
- Position sensitivity levels for some users were incorrect based on their job function

INDEPENDENT AUDITORS' REPORT (Continued)
EXHIBIT A
Significant Deficiency

Access controls

- User access was not always granted in accordance with the principle of least privilege
- Termination of system access for separated employees and contractors was not always completed timely
- Inactive accounts were not always disabled
- Certain users had access to application development and production environments
- User access was not always recertified

Configuration management

- System configuration settings were not always in compliance with FSA policy
- System change testing was not always documented

These deficiencies can increase the risk of unauthorized access to the Department and FSA's systems used to capture, process, and report financial transactions and balances, affecting the reliability and security of the data and information. These findings are discussed in further detail below and in a Limited Distribution Report provided to the Department and FSA management.

Security management

An effective information security management program should have a framework and process for assessing risk, effective security procedures, and processes for monitoring and reporting the effectiveness of these procedures. We noted the Department's information security policies were outdated or did not fully address specific controls required by NIST Special Publication (SP) 800-53, Revision 4, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations*.¹ For two systems, we noted their System Security Plans' control baselines were based on NIST SP 800-53, Revision 3. NIST SP 800-53, Revision 4 was published in 2013 with an April 1, 2014 implementation deadline for executive agencies.

Additionally, two systems were given Authority to Operate (ATO) memoranda prior to the completion of security assessment and authorization (SA&A) activities. Although an assessment of the design of controls was conducted in 2013, the last security control assessment that determined the extent to which the controls were implemented and operating as intended was completed in 2010. As such, the most recent system risk assessment was completed in 2010. Therefore, the ATOs were issued without the review of a complete and timely security assessment and authorization package as required by NIST SP 800-37, Revision 1 *Guide for Applying the Risk Management Framework to Federal Information Systems*, resulting in an

¹ NIST SP 800-53 revision 4 was issued in April 2013. According to the Office of Management and Budget (OMB) memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* requires that for non-national security programs and information systems, agencies must follow NIST standards and guidelines. For legacy information systems, agencies are expected to be in compliance with NIST standards and guidelines within one year of the publication date unless otherwise directed by OMB. The one year compliance date for revisions to NIST publications applies only to the new and/or updated material in the publications.

INDEPENDENT AUDITORS' REPORT (Continued)
EXHIBIT A
Significant Deficiency

increased risk that the Authorizing Official, Information System Security Officers (ISSOs), and system owners were not informed of the ongoing security issues and risks to these systems.

With regard to corrective action of system control weaknesses, we noted that the Plans of Action and Milestones (POA&Ms) for one system had passed their scheduled dates of completion without documented justification for missed completion dates or adjusted expected completion dates. Additionally, we noted POA&Ms that did not have a documented mitigation strategy. We also noted that the corrective action of certain control weaknesses discovered through vulnerability scanning of another system was not being formally tracked through its remediation. Without formally documenting each remediation plan, along with the estimated dates of completion and status of corrective actions, management cannot ensure weaknesses are remediated effectively or timely.

Finally, for two of the five systems tested, we noted system users did not always complete the required security awareness training. Also, individuals with significant system security responsibilities had not always completed role based training for these systems.

Personnel Security

Personnel security involves screening individuals before granting them access to computer resources commensurate with the risk and magnitude of the harm the individual could cause. We found background reinvestigations were not being tracked effectively and position sensitivity levels were not always commensurate with the users' current job duties. Specifically, we noted the following for a sample of individuals with significant system security responsibilities:

- Lack of evidence of an investigation or users with overdue reinvestigations
- Investigation levels lower than the level required by the users' access requirements and responsibilities
- Lack of sensitivity level documentation for users or sensitivity level documentation lower than the level required for a users' access requirements and responsibilities

Access Controls

Access controls limit or detect inappropriate access to systems, protecting the data within them from unauthorized modification, loss or disclosure. Agencies should have formal policies and procedures for controlling access to information systems and related control activities should be properly implemented and monitored. One key element of access control is *boundary protection*. Properly managed interfaces between FSA systems and external parties help reduce the risk of unauthorized access. NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, specifies that an agreement should be documented for the interconnection between organizations. A Memorandum of Understanding (MOU) documents the terms and conditions for sharing data and information resources in a secure method. An Interconnection Security Agreement (ISA) identifies the technical and security requirements for establishing, operating, and maintaining the interconnection and supports the MOU. We identified expired MOUs and instances in which interconnections were not detailed in the System Security Plan for one system.

User authorization refers to the documentation of the granting of user access to only the elements of a system the user needs to perform his or her duties. To be an effective control, user access should be documented, approved and periodically reviewed. Accounts for users

INDEPENDENT AUDITORS' REPORT (Continued)
EXHIBIT A
Significant Deficiency

should be terminated when the user no longer needs access to the system. Based on our work, we noted:

- Accounts for terminated employees and contractors were not disabled for three of the four systems tested
- Inactive accounts were not disabled for two systems
- For one system, an individual was granted an inappropriate level of system access
- User access recertification was not fully completed for three systems
- Certain users had inappropriate access to one system's development and production environments

Configuration Management

Configuration management ensures changes to systems are tested and approved, and systems are configured securely in accordance with policy. In our audit, we found two systems with configuration settings that were not in compliance with FSA's policy and one system with configuration settings that were not in compliance with Department's policy. Additionally, we could not obtain evidence of testing related to a sample of changes for one system. This was primarily due to testing documentation not being maintained in the change management ticketing system.

The Department's Chief Information Officer FY2014 Federal Managers' Financial Integrity Act of 1982 (FMFIA) Assurance Letter reported control deficiencies related to access controls and contingency planning. In addition, FSA's FY2014 FMFIA Assurance Letter reported control deficiencies related to access controls and configuration management. Also, the Department's FY2014 Federal Information Security Management Act (FISMA) review identified control deficiencies in six of eleven reporting metrics related to the following areas: configuration management, identity and access management, incident response and reporting, risk management, remote access management, and contingency planning. In addition, five of the 11 reporting metrics contained repeat or modified repeat findings from reports issued from the last three years.

These deficiencies can increase the risk of unauthorized access to the Department's systems used to capture, process, and report financial transactions and balances.

NIST Special Publication 800-39, *Managing Information Security Risk - Organization, Mission, and Information System View*, states:

"The complex relationships among missions, mission/business processes, and the information systems supporting those missions/processes require an integrated, organization-wide view for managing risk. Unless otherwise stated, references to risk in this publication refer to information security risk from the operation and use of organizational information systems including the processes, procedures, and structures within organizations that influence or affect the design, development, implementation, and ongoing operation of those systems. The role of information security in managing risk from the operation and use of information systems is also critical to the success of organizations in achieving their strategic goals and objectives. Historically, senior leaders/executives have had a very narrow view of information security either as a technical matter or in a stovepipe that was independent of organizational risk and the traditional management and life cycle processes. This extremely limited perspective

INDEPENDENT AUDITORS' REPORT (Continued)
EXHIBIT A
Significant Deficiency

often resulted in inadequate consideration of how information security risk, like other organizational risks, affects the likelihood of organizations successfully carrying out their missions and business functions. This publication places information security into the broader organizational context of achieving mission/business success. The objective is to:

- Ensure that senior leaders/executives recognize the importance of managing information security risk and establish appropriate governance structures for managing such risk;
- Ensure that the organization's risk management process is being effectively conducted across the three tiers of organization, mission/business processes, and information systems;
- Foster an organizational climate where information security risk is considered within the context of the design of mission/business processes, the definition of an overarching enterprise architecture, and system development life cycle processes; and
- Help individuals with responsibilities for information system implementation or operation better understand how information security risk associated with their systems translates into organization-wide risk that may ultimately affect the mission/business success.

To successfully execute organizational missions and business functions with information system-dependent processes, senior leaders/executives must be committed to making risk management a fundamental mission/business requirement. This top-level, executive commitment ensures that sufficient resources are available to develop and implement effective, organization-wide risk management programs. Understanding and addressing risk is a strategic capability and an enabler of missions and business functions across organizations. Effectively managing information security risk organization-wide requires the following key elements:

- Assignment of risk management responsibilities to senior leaders/executives;
- Ongoing recognition and understanding by senior leaders/executives of the information security risks to organizational operations and assets, individuals, other organizations, and the Nation arising from the operation and use of information systems;
- Establishing the organizational tolerance for risk and communicating the risk tolerance throughout the organization including guidance on how risk tolerance impacts ongoing decision-making activities; and
- Accountability by senior leaders/executives for their risk management decisions and for the implementation of effective, organization-wide risk management programs."

The ineffective and untimely remediation of application control weaknesses and repeat deficiencies identified across multiple applications indicates the need for improved strategic IT management.

In recognition of the need to improve internal control related to information security, the Department and FSA CISOs continue to work together to put a framework in place for more effectively managing system security risk by reviewing control weaknesses across the organization, determining their root cause, and tracking remediation activities. The security

INDEPENDENT AUDITORS' REPORT (Continued)
EXHIBIT A
Significant Deficiency

posture of the systems is reviewed on a monthly basis by reviewing control weaknesses noted from audits, self assessments, vulnerability scans, and associated POA&Ms. In addition, the Department updated and approved OCIO-1, *Information Assurance/Cybersecurity Policy*, which provides policy guidance from the OCIO for all IT assets and services operated within or on behalf of the Department. Underlying security procedures and guidance documentation is in the process of being updated. The Department also completed the implementation of a Security Operations Center allowing for security issues to be centrally tracked and managed for the Department and FSA. The Department has continued to make progress on implementing a risk management framework for applying continuous system monitoring based on NIST SP 800-37 with a scheduled completion date of FY2015. Furthermore, the Department refined the service-level agreements for the IT general support system contract to increase accountability of the service provider for remediating system control issues. FSA is working on a plan to review selected IT security controls at all Guaranty Agencies (GAs) within a two year period. FSA has already been assessing the IT security controls at the Title IV Additional Servicers (TIVAS) and Private Collection Agencies (PCAs) in order for the CISO to issue an ATO. These activities show progress and commitment from the Department and FSA senior managers to strengthen system security controls across the Department and FSA.

In order to fully implement an agency-level program for monitoring compliance with the information security program, the procedures and guidance supporting the Information Assurance/Cybersecurity Policy need to be completed, approved and disseminated in order to define the agency-wide information security program and practices. Without comprehensive current information security policies and procedures, there is an increased likelihood that information security may not be addressed throughout the lifecycle of the Department and FSA's information systems. Moreover, employees and contractors may be performing tasks without clear direction or training. Due to the continuance of persistent IT control deficiencies across multiple systems, the CISOs need to continue to refine the process for ensuring accountability of the Department and FSA system owners, ISSOs, contractors, and FSA's Technology Office and Business Operations responsible for the security, operation and maintenance of the Department and FSA systems to remediate control deficiencies.

Recommendations:

We recommend the Department CISO work with the FSA CISO to:

- 1a. Refine and fully implement FSA's system security program to monitor compliance with NIST requirements, in coordination with the Department's organization wide information security program, at both the agency and system level.
- 1b. Implement a process to ensure accountability for individuals responsible for remediating the identified control deficiencies in the Department and FSA's systems, including cooperation between the Technology Office and Business Operations.
- 1c. Implement a process for holding contractors accountable for remediation of control deficiencies in the Department and FSA's systems.

INDEPENDENT AUDITORS' REPORT (Continued)
EXHIBIT B
Instance of Noncompliance

Noncompliance with Title 31 United States Code (U.S.C.) Section 3716(c)(6)

Title 31 U.S.C. Section 3716(c)(6) states that any Federal agency that is owed by a person a past due, legally enforceable nontax debt that is over 180 days delinquent, including nontax debt administered by a third party acting as an agent for the Federal Government, shall notify the Secretary of the Treasury of all such nontax debts for purposes of administrative offset under this subsection.

The Digital Accountability and Transparency Act (DATA Act), Public Law 113-101, was signed into law on May 9, 2014. Section 5 of the DATA Act amends Title 31 U.S.C. Section 3716(c)(6) and now requires agencies to notify the Secretary of the Treasury of valid, delinquent nontax debts that are over 120 days delinquent – 60 days earlier than the previous 180 days requirement – for the purpose of administrative offset. Section 5 of the DATA Act also added a new requirement, according to which “the Secretary of the Treasury shall notify Congress of any instance in which an agency fails to notify the Secretary [of the Treasury] as required” by 31 U.S.C. Section 3716(c)(6)(A).²

The Department and FSA have not changed their loan servicing procedures and internal processes to comply with the new 120 days requirement. Further, the existing loan servicing procedures and internal processes do not notify the Secretary of the Treasury of past due, legally enforceable nontax debts once they become over 180 days past due. Instead, notification is performed once a year when most past due, legally enforceable nontax debts are significantly older than 180 days delinquent. Therefore, the Department and FSA are noncompliant with the timing requirement of 31 U.S.C. Section 3716(c)(6) as of September 30, 2014.

Recommendation:

We recommend that the Secretary of Education and FSA Chief Operating Officer:

2. Revise their loan servicing procedures and internal processes to comply with the timing requirement of Title 31 U.S.C. Section 3716(c)(6), as amended by the DATA Act.

² The official U.S.C has not yet been amended to reflect the statutory change due to the passage of the DATA Act.

INDEPENDENT AUDITORS' REPORT (Continued)
EXHIBIT C
Management's Response



UNITED STATES DEPARTMENT OF EDUCATION
 OFFICE OF THE CHIEF FINANCIAL OFFICER

MEMORANDUM

NOV - 7 2014

TO: Kathleen S. Tighe
 Inspector General

FROM: Thomas P. Skelly *Thomas P. Skelly*
 Delegated to Perform the Functions
 and Duties of the Chief Financial Officer

Danny A. Harris, Ph.D. *Danny A. Harris*
 Chief Information Officer

SUBJECT: DRAFT AUDIT REPORTS
 Fiscal Years 2014 and 2013 Financial Statements
 U.S. Department of Education
 ED-OIG/A1700001

Please convey our sincere thanks and appreciation to everyone on your staff who worked diligently on this financial statement audit. The Department reviewed the draft Fiscal Years 2014 and 2013 Financial Statement Audit Report. We concur and agree with the Independent Auditors' Report.

We will share the final audit results with responsible senior officials, other interested program managers, and staff. At that time, we will also request the preparation of corrective action plans to be used in the resolution process.

Again, please convey our appreciation to everyone on your staff whose efforts permitted the Department to complete the audit within the established timeframe.

Please contact Gary Wood, Director, Financial Management Operations, at (202) 245-8118 with any questions or comments.

400 12th St. S.W., WASHINGTON, DC 20202
 www.ed.gov

The Department of Education's mission is to promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access.

INDEPENDENT AUDITORS' REPORT (Continued)
EXHIBIT D
Status of Prior Year Recommendations

Our assessment of the current status of the recommendations related to findings identified in the prior year audit is presented below:

Fiscal Year 2013 Recommendation	Fiscal Year 2014 Status
Significant Deficiency 1- <i>Functionality and Internal Controls over Some Loan Servicing Systems Need Improvement</i>	
CLA recommended that the Chief Operating Officer of FSA:	
1a. Ensure all servicing application functionality is corrected to meet the Department's requirements for servicing loans and reporting financial activity and balances timely and accurately.	One of the systems was decommissioned. Significant functionality issues for the other system were addressed. Minor remaining and new issues reported in the management letter.
1b. Continue to monitor the scheduled transfers of defaulted loans to DMCS and ensure that all new loan servicers are fully set up to transfer defaulted loans to the defaulted loan servicer.	Significant functionality issues relating to transfers addressed and the transfer backlog was significantly reduced. Minor remaining and new issues reported in the management letter.
1c. Continue to correct loan balances affected by the functionality issues and properly inform the impacted borrowers of the corrected account balances.	Corrective action to adjust immaterial errors in account balances will continue into FY2015. Remaining issues reported in the management letter.
1d. Continue to monitor servicers' efforts to reduce the balance of unposted cash transactions, unrecorded borrower transactions, and general ledger posting differences, including the posting of transfer transactions in and out of DMCS.	One of the systems was decommissioned. The effect of the remaining issues in the other system was immaterial throughout FY2014. Recommendation made in the management letter.
1e. Establish protocols for management approval for write-offs and manual adjustments of unresolved differences once corrective actions are no longer cost effective.	Management implemented a protocol to approve write-offs and manual adjustments arising from the corrective actions that address the system functionality issues. Resolved.
1f. Continue to monitor the timeliness and accuracy of account reconciliations prepared by the servicers.	Improvement noted during FY2014. Recommendation to continue monitoring new contractor noted in management letter.

INDEPENDENT AUDITORS' REPORT (Continued)
EXHIBIT D
Status of Prior Year Recommendations

Significant Deficiency 2 - Department and FSA Management Need to Mitigate Persistent Information Technology (IT) Control Deficiencies	
CLA recommended that the Department and FSA CISOs:	
2a. Refine and fully implement the program to monitor compliance with the Department's organization-wide information security program and NIST requirements at the Department and system level.	Progress was made, however corrective action is still in process; see Significant Deficiency
2b. Implement a process ensuring accountability for individuals responsible for remediating the identified control deficiencies in the Department and FSA's systems, including cooperation between the Technology Office and Business Operations.	Progress was made, however corrective action is still in process; see Significant Deficiency
2c. Implement a process for holding contractors accountable for remediation of control deficiencies in the Department and FSA systems.	Progress was made, however corrective action is still in process; see Significant Deficiency
2d. Implement a process for holding third party service providers accountable for the remediation of control deficiencies associated with their information systems.	Resolved
Noncompliance with Laws and Regulations	
The Department's Financial Management Systems Do Not Meet Federal Financial Management Systems Requirements	Resolved, as the key system contributing to noncompliance was decommissioned and the other system was significantly improved.