

REPORT OF THE INDEPENDENT AUDITORS



UNITED STATES DEPARTMENT OF EDUCATION OFFICE OF INSPECTOR GENERAL

THE INSPECTOR GENERAL

November 13, 2017

The Honorable Betsy DeVos
Secretary of Education
Washington, D.C. 20202

Dear Secretary DeVos:

The enclosed report presents the results of the audit of the U.S. Department of Education's (Department) financial statements for fiscal years 2017 and 2016 to comply with the Chief Financial Officers Act of 1990, as amended. The report 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, 2017 and 2016, 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 2017 and 2016 financial statements are presented fairly, in all material respects, in accordance with accounting principles generally accepted in the United States of America;
- Two significant deficiencies in internal control over financial reporting:
 - Controls over the Department's Modeling Activities Need Improvement, and
 - Department and Federal Student Aid Management Need to Mitigate Persistent Information Technology Control Deficiencies; and
- One instance of reportable noncompliance with Federal law related to referring delinquent student loan debts to Treasury.

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

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 Betsy DeVos

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.

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 comply with the Federal Financial Management Improvement Act of 1996, or on compliance with certain provisions of laws, regulations, contracts, and grant agreements.

CliftonLarsonAllen is responsible for the enclosed independent auditors' report and the conclusions expressed on internal control and compliance. 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 report, 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 consolidated financial statements of the United States Department of Education (Department), which comprise the consolidated balance sheets as of September 30, 2017 and 2016, and the related consolidated statements of net cost and changes in net position, and the combined statement of budgetary resources for the years then ended, and the related notes to the consolidated 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.); this includes 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. 17-03, *Audit Requirements for Federal Financial Statements* (OMB Bulletin 17-03). Those standards and OMB Bulletin 17-03 require that we plan and perform the audits 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

INDEPENDENT AUDITORS' REPORT (Continued)

of accounting policies used and the reasonableness of 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.

Opinion on the Financial Statements

In our opinion, the consolidated 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, 2017 and 2016, 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. require that the information in the Management's Discussion and Analysis (MD&A), Required Supplementary Information (RSI), and Required Supplementary Stewardship Information (RSSI), included in the U.S. Department of Education's FY 2017 Agency Financial Report, be presented to supplement the financial statements. Such information, although not a part of the financial statements, is required by the Federal Accounting Standards Advisory Board, 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, 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 audits 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

Our audits were conducted for the purpose of forming an opinion on the financial statements as a whole. The Message from the Secretary, Message from the Chief Financial Officer, Other Information, and Appendices in the U.S. Department of Education FY 2017 Agency Financial Report are presented for purposes of additional analysis and are not a required part of the financial statements or RSI. In addition, management has included references to information on websites or other data outside of the Agency Financial Report. This information has not been subjected to the auditing procedures applied in the audits 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 on Compliance Based on an Audit of Financial Statements Performed in Accordance with *Government Auditing Standards*

Internal Control over Financial Reporting

In planning and performing our audit of the consolidated 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 statement of 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. However, we identified certain deficiencies in internal control, described below and in more detail in Exhibit A, which we consider to be significant deficiencies.

Controls over the Department's Modeling Activities Need Improvement

The Department maintains various models that apply mathematical techniques or statistical methods to historical student loan event data to estimate future loan performance and calculate the cost or value of the various student loan programs on a present value basis. In FY2016, we identified deficiencies in the controls over, and documentation of, the Department's processes for model design and development, risk assessment, model operation and validation, and oversight. We also identified certain deficiencies in the Department's modeling for income-driven repayment (IDR) loans.

In FY2017, the Department implemented corrective actions to improve its controls over modeling activities, including the enhancement of the scope and responsibilities of the Credit Reform Working Group, the development of a model inventory and preliminary risk assessment. However, the Department's FY2017 model validation procedures identified potential areas for model enhancements that require additional analysis. The Department does not have a formal structure to capture and track these issues identified in their model risk assessment document.

INDEPENDENT AUDITORS' REPORT (Continued)

The Department also made a number of technical model revisions to address findings identified by the Government Accountability Office in FY2016, but corrective actions for certain other issues, including income imputation for IDR loans, are still in process.

They also initiated other corrective actions that have not yet been completed, including the development of policies and procedures for model development, operation and validation, and performance of an independent validation of the Student Loan Model. These remaining issues could impact the reliability of the subsidy estimates used for financial reporting, budgetary formulation and management analysis.

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

The Department oversees a large portfolio of Department-owned and contractor-owned business systems and applications that requires an effective and comprehensive information system security program. Prior audits have identified numerous control deficiencies at the Department, Federal Student Aid (FSA), and application level. This year, the Department made substantial progress in completing entity-wide information security policies and procedures and addressing general application control deficiencies for the Department's core financial management system. However, we continued to identify control deficiencies in the Department's information security program relating to personnel management and compliance monitoring. We also found configuration management weaknesses in the Department's general network and core financial management system. Furthermore, we continued to identify general control deficiencies in FSA's financial applications. These deficiencies 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 its data and information.

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 discussed in the second paragraph below, disclosed one instance of noncompliance, described below and in Exhibit B, which is required to be reported in accordance with *Government Auditing Standards* and OMB Bulletin 17-03.

As of September 30, 2017, FSA is not in compliance with the legal requirement for referring 120 day delinquent student loan debts to Treasury. In 2014, Federal law¹ was amended² to require agencies to notify the Secretary of the Treasury of valid, delinquent nontax debts that are over 120 days delinquent – 60 days earlier than

¹ 31 U.S. Code Section 3716(c)(6)

² Public Law 113-101 (DATA Act) Section 5

INDEPENDENT AUDITORS' REPORT (Continued)

the previous 180 days requirement – for the purpose of administrative offset (i.e. collection through the reduction of future Federal payments). Due to the number of entities and systems involved in handling student loan debts, FSA is not yet capable of meeting this accelerated timeline.

We also performed tests of compliance with certain provisions of the Federal Financial Management Improvement Act (FFMIA). 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 these provisions 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.

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 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 to certain provisions of laws, regulations, contracts and grant agreements noncompliance with which could have a direct effect on the determination of material financial statement amounts and disclosures. 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 FFMIA would not necessarily disclose all instances of noncompliance with FFMIA requirements.

INDEPENDENT AUDITORS' REPORT (Continued)***Management's Response to Findings***

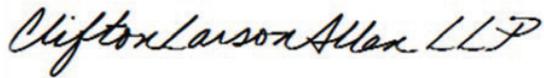
Management's response to the findings identified in our report is presented in Exhibit C. We did not audit the Department's response and, accordingly, we express no opinion on it.

Status of Prior Year's Control Deficiency and Noncompliance Issue

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 November 14, 2016. The status of prior year findings is presented in Exhibit D.

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

The purpose of the Report on Internal Control over Financial Reporting and on Compliance 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 13, 2017

INDEPENDENT AUDITORS' REPORT (Continued)
EXHIBIT A
Significant Deficiencies

Controls over the Department's Modeling Activities Need Improvement

The Department does not have a fully developed framework for model risk management and governance, or fully developed internal controls over its critical modeling activities, including model development, risk assessment, operation, and validation.

The Cost Estimation and Analysis Division (CEAD), a component of the Department's Office of Planning, Evaluation and Policy Development, is responsible for developing estimates of the subsidy cost of the Department's direct and guaranteed loan programs. These estimates are used to support budget estimates, policy decisions and financial reporting. CEAD has developed a set of complex financial and economic models that apply mathematical techniques and statistical methods to historical loan level data to develop student loan program performance assumptions and estimate the value and cost of the Department's various loan programs. These models also support management's estimate of the net present value of cash flows related to nearly \$1.4 trillion in direct, defaulted, and guaranteed student loans as of September 30, 2017.

An effective control structure is generally defined through appropriately documented, approved, and implemented policies and procedures that outline requirements for ensuring all modeling and related control activities are performed and documented in accordance with the intent of management. A proper governance structure involves input from program management and multiple layers of review, approval, and oversight from CEAD management, the Department and FSA Offices of the Chief Financial Officer, and senior agency management over modeling activities. Our audit identified the following:

Model development

The Department does not have a formalized process for managing critical model development and configuration management activities, which should include authorization; defining the objectives, applicable program attributes, and requirements affecting the planned model; evaluation of available data; proposed design and potential design alternatives; and model testing, approval, and implementation.

Our FY2016 audit found the Department maintained limited documentation supporting the initial design, evaluation, justification and testing of the models for:

- selecting a sample of borrowers from the National Student Loan Data System (NSLDS) used for calculating program performance assumptions
- estimating future incomes for borrowers under income-dependent repayment plans
- projecting future cash flows for borrowers under income-dependent repayment plans
- calculating specific performance assumptions
- projecting overall program level cash flows (Student Loan Model)

During FY2016, CEAD updated its model for recoveries on defaulted loans and enhanced documentation related to the NSLDS sampling process. In FY2017, CEAD updated their model for prepayments and loan forgiveness due to death, disability, and bankruptcy, and have begun efforts to update their model for defaults. CEAD also implemented a number of enhancements to their income-driven repayment (IDR) model in response to deficiencies identified in a FY2016 GAO report. These included incorporating inflation factors to income forecasts, adjusting grouping factors for imputed borrower incomes to reduce income volatility, and modifying the IDR participation allocation rates related to parent PLUS loans, which are not eligible for IDR. Their

INDEPENDENT AUDITORS' REPORT (Continued)
EXHIBIT A
Significant Deficiencies

documentation for these modifications represented a significant improvement in discussing the methodology and their basis. However, the documentation was not sufficiently detailed to serve as a fully effective guide for an independent reviewer to follow the procedures performed.

The Department performs data quality reviews of its primary data source used in its modeling activities (the National Student Loan Data System or NSLDS). However, the Department does not have a structured process to document its evaluation of whether the reviews sufficiently address the specific data used within its models, or independently determine the appropriateness or reliability of the data used by their models. The Department also does not have a structured process for implementing, controlling and securing the various versions of the models maintained.

CEAD has begun discussing these actions with the Department's reconstituted modeling oversight group, the Credit Reform Working Group (CRWG), in its monthly meetings, but does not document their model development plan, testing plans and approval of testing results before changes are implemented.

CEAD is comprised of a small team of experienced economists and analysts responsible for performing its modeling activities, and thoroughly documenting such design requirements, development processes, and testing evaluation is onerous for the current team. The Department has obtained additional contract support to assist with these efforts, but did not approve an additional specialist position for CEAD. Given the size, growth and changes of the Direct Loan Program in recent years, ineffective controls over the design of new models can significantly impact the reliability of their estimates.

Model risk assessment

CEAD maintains over 18 different economic and financial modeled assumptions used within the calculation of the Allowance for Subsidy for the Direct Loan Program and various other model assumptions for the FFEL and other Department programs. Some of the assumptions are updated annually, while others are updated biannually. The Department does not have a formalized process for maintaining the Department's model inventory, accumulating, assessing and documenting modeling risks, and monitoring the modification or development of its models. This risk assessment process should be independent of the agency-level risk assessment process performed in connection with the agency level management controls review process required by OMB Circular A-123, and should assist the CRWG in supporting the prioritization of model development activities within the normal CEAD workload. In FY2017, the Department has initiated an independent, external validation review of its models.

Model operation

The Department's documentation of the control activities performed for operating approved models is not formalized. We identified deficiencies in the documentation of control activities over the Department's model operations relating to data accumulation and validation, assumption development, and model execution. As a result, we could not verify the operating effectiveness of certain control activities, including various reviews and approvals. Although the Department completed technical documentation of the Student Loan Model (SLM) in FY2017, their documentation of policies and procedures remains incomplete.

INDEPENDENT AUDITORS' REPORT (Continued)
EXHIBIT A
Significant Deficiencies

Model validation

Model validation refers to the initial and ongoing review and approval of the design of the model and its ability to properly correlate historical data into estimated future program performance. The Department performs a number of critical procedures to monitor the performance of its models and validate the overall reasonableness of its outputs, including backcasts, cash flow analyses, and sensitivity analyses. However, these procedures are performed at the aggregate level and the Department does not evaluate the performance of specific cash flows, assumptions or individual models against established benchmarks using sound approaches and statistical measures of performance. We identified opportunities to enhance the usefulness of various monthly accounting reports that are reviewed by the CRWG and could serve to identify unusual program activity or other potential modeling issues.

The Department also does not have a process to comprehensively evaluate the results of these procedures and document their conclusion as to whether the models, in aggregate, continue to be adequate for forecasting the future performance of the student loan programs.

Governance

In FY2017, the Department formalized the roles and responsibilities of the CRWG, which includes various members of Department and FSA management, and serves as the first level monitoring structure over the Department's modeling activities. Due to the current status of the Department's enterprise risk management program, the CRWG has been unable to initiate efforts to integrate model risk issues with Department's risk management program.

Summary

Without a fully effective risk management and control structure over its modeling activities, estimation errors or modeling risks may go undetected, increasing the potential for improper reporting and program decisions.

GAO's *Standards for Internal Controls in the Federal Government* requires that agencies:

- design controls activities in response to objectives and risks
- define and delegate responsibilities
- document internal controls and "all transactions and other significant events"
- evaluate and document the results of ongoing monitoring evaluations to identify internal control issues

OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, updated in July 2016, requires agencies to take steps to integrate risk management into the internal controls over their business operations.

Industry specific guidance from federal regulators regarding model risk management, model governance and related controls is also provided by the Federal Reserve and the Office of the Comptroller of the Currency in Supervision and Regulation (SR) 11-7, *Supervisory Guidance on Model Risk Management*, and by the Federal Housing Finance Agency in their AB 2013-07 *Model Risk Management Guidance*.

INDEPENDENT AUDITORS' REPORT (Continued)
EXHIBIT A
Significant Deficiencies

Recommendations:

We recommend the Director, Budget Service:

- 1a. Develop and document the Department's process, policies and procedures for the authorization, design, development, testing, approval and implementation of new models and model enhancements.
- 1b. Document the Department's process, policies, procedures and related controls for managing the operation and use of approved models.
- 1c. Enhance the process to capture model risks, update the assessment of risks related to each model, and document how that assessment impacts the Department's prioritization of corrective actions, and requisite level of controls, validation and monitoring over each model.
- 1d. Document and enhance the Department's processes, policies, procedures and related controls for the periodic review, validation and approval of the Department's models at the assumption, model and program level.
- 1e. Document the overall review and conclusions drawn related to the evaluation of the results of model performance reviews and validation procedures performed.
- 1f. Ensure modeling risks are considered in connection with the Department's enterprise risk management program.

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

The Department oversees a large portfolio of Department-owned and contractor-owned business systems and applications that requires an effective and comprehensive information system security and privacy program. According to OMB Circular A-130, *Managing Information as a Strategic Resource*, key elements of an effective security program include 1) agency-wide and system-level policies and procedures; 2) properly designed, implemented and monitored information system controls to protect Department information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction; and 3) cost effective risk management.

Prior audits have identified numerous control deficiencies at the Department and application level. While the Department has made gradual progress to address these issues in recent years, we continued to identify certain control deficiencies in the Department's information security program relating to compliance monitoring, personnel management, and management of various application level security, configuration management, and access controls. In addition, we continued to identify general application control deficiencies in FSA's financially relevant applications.

Effective system security starts with strong governance, including agency level oversight, policies and procedures, entity-wide controls, and controls monitoring. We have reported for several years that the Department's agency level information technology policies were outdated or did not fully address specific controls required by National Institute of Standards and Technology (NIST) guidance. Designing and implementing effective agency level policies is the responsibility of the Department's Chief Information Officer (CIO). This year the CIO substantially completed the guidance associated with the Department's Information Assurance/Cybersecurity Policy.

INDEPENDENT AUDITORS' REPORT (Continued)
EXHIBIT A
Significant Deficiencies

Managing the information and system security program across the Department is primarily the responsibility of the Department's Chief Information Security Officer (CISO), in conjunction with FSA's CISO. The Department and FSA CISOs have enhanced their efforts to monitor the system security control activities over their agency systems in recent years and have initiated several multi-year corrective actions that should aid in addressing many of the long standing weaknesses that affect the Department and FSA systems. For example, the FSA CISO has implemented a security program based on continuous monitoring that includes regular updates to security documentation, routine security control assessments and vulnerability assessments, and risk analysis. The outcomes of these system security activities are reviewed and evaluated by the CISO in support of an ongoing authorization to operate. Monitoring of remediation activities associated with identified control deficiencies in FSA's systems is fostered by regular update meetings held with management within the Technology Office and Business Operations, the Office of Inspector General (OIG) and the financial statement auditors.

However, agency-level security controls also require the efforts of other offices across the Department, including the Office of Security, Facilities and Logistics Services. We continue to find a large number of Department employees and contractors with overdue reinvestigations, incorrect levels of background investigations for privileged users, and lack of investigation information. In addition, although the Department provided training for completing position designations using the Office of Personnel Management's Position Designation Tool, the Department's Office of Management has not ensured Department system owners completed position designations in order to determine and document suitability and investigation requirements for each system's roles/responsibilities. Furthermore, the Department CISO has been working with Contracting on language for service level agreements (SLAs) for contractor employee clearance monitoring as recommended in FY 2015, however the SLAs have not yet been implemented.

The Department's agency-level information security controls are required to be evaluated annually by the OIG, in accordance with the Federal Information Security Modernization Act (FISMA). The FY 2016 OIG review involved testing financial and non-financial systems' controls and identified control deficiencies in five of eight reporting areas related to configuration management, information security continuous monitoring, incident response, identity and access management, and security and privacy training.

Although FSA implemented a governance structure for managing agency-level system security risk, the tactical execution of remediating system level control weaknesses and ensuring compliance with information security requirements still needs improvement.

Managing system security controls at the application or system level is the responsibility of the system owners, in conjunction with system level information system security officers (ISSOs). Since last year, FSA added additional ISSOs and an ISSO supervisor; however, our audit continued to identify application, or system, specific control deficiencies in the areas of security management, access controls, configuration management, and contingency planning in one or more of the five financial systems we tested this year. We continued to identify configuration management issues with the Department's general support system, but noted substantial improvement in the remediation of information security control weaknesses for the Department's core financial management system.

At FSA, we tested four systems and our audit continued to identify control deficiencies in security management, access controls, configuration management, and contingency planning across

INDEPENDENT AUDITORS' REPORT (Continued)
EXHIBIT A
Significant Deficiencies

these systems. The agency expected to implement a new system for user access management to address various access control deficiencies this year, but this system was not completed.

Specifically, we identified system specific issues in the following areas:

Security management

- Plans of Action and Milestones (POA&Ms) were not updated with the results from security control assessments or vulnerability assessments for two FSA systems, and POA&Ms were not updated on a quarterly basis for four FSA systems
- Role based security training for users with significant system security responsibilities was not always completed for one FSA system tested
- Interconnection agreements were not detailed in System Security Plans and/or were not current for one FSA system
- Background reinvestigations were not tracked adequately or completed timely; and inappropriate levels of investigations were completed for numerous Department and FSA employees and contractor users
- Position designations were not finalized for Department employees and contractors
- Evidence to validate Department assets were returned for separated Department employees was not always provided

Access controls

- User access for one FSA system was not always approved for all roles granted
- Termination of system access for separated employees and contractors was not always completed timely for three FSA systems
- Inactive accounts were not always disabled for one FSA system
- User access for three FSA systems was not always recertified and some user accounts that were recertified had either never used the system, or had not logged in for an extended period of time

Configuration management

- System configuration settings were not always compliant with Department policy for one FSA system
- Computer security configurations were inadequate and software was not patched or was unsupported for two Department systems

Contingency Planning

- Contingency plan tests were not conducted annually for one FSA system

The combination of agency-level and system specific 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 to be provided to the Department and FSA management.

INDEPENDENT AUDITORS' REPORT (Continued)
EXHIBIT A
Significant Deficiencies

Security management

An organization-wide information security program sets the framework for addressing risk through developing and implementing effective information security procedures, monitoring the effectiveness of those procedures, providing appropriate security training and remediating control weaknesses through the POA&M process. Security policies and procedures also include employee hiring, transfer and termination practices.

Overall, we found improvement in the level of compliance with security awareness training requirements this year. For one FSA system, we found system users with significant system security responsibilities had not always completed role based training.

In addition, documentation was not provided to validate that Department assets were returned and access was disabled timely for one of 25 separated employees tested. In addition evidence was not provided to validate that Personal Identity Verification cards were returned for the entire population of 25 separated employees tested. Furthermore, we noted issues with regard to background investigations, including numerous individuals with overdue investigations, privileged users with an incorrect level of investigation based on their system access and job function, and privileged users without documented background investigation status.

Access Controls

Access controls limit or detect inappropriate access to systems, protecting the data within them from unauthorized modification, loss or disclosure. Standards require that entities use a properly executed Memorandum of Understanding (MOU) to document 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. Consistent with previous years, for one system, we identified expired MOUs, and instances in which interconnections were not detailed in the corresponding System Security Plan.

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

- Accounts for terminated FSA, and loan servicer employees were not disabled for three of the four FSA systems tested
- Inactive accounts were not disabled for one FSA system
- For one FSA system, one from a sample of 25 new users did not have evidence that all user roles were approved
- User access for three systems was not always recertified, and some user accounts that were recertified for one system had either never used the system, or had not logged in for an extended period of time

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 one FSA system with configuration settings that did not adhere to Department policy. Furthermore, our testing identified insecure configurations, as well as unpatched and unsupported software for two systems.

INDEPENDENT AUDITORS' REPORT (Continued)
EXHIBIT A
Significant Deficiencies

Contingency Planning

Contingency plan tests were not conducted annually for one FSA system.

Information Security Program

The OIG performs an independent evaluation of the Department's information technology security program and practices, as required by the Federal Information Security Modernization Act of 2014 (FISMA). The 2017 FISMA evaluation identified findings in all seven areas reviewed: (1) Risk Management, (2) Configuration Management, (3) Identity and Access Management (4) Security Training, (5) Information Security Continuous Monitoring, (6) Incident Response, and (7) Contingency Planning. The report made 37 recommendations (4 of which were repeat recommendations) to assist the Department and FSA with increasing the effectiveness of their information security program.

According to NIST SP 800-39, *Managing Information Security Risk - Organization, Mission, and Information System View*, the information system owner, in coordination with the information system security officer, is responsible for ensuring compliance with information security requirements.

The information system security officer is an individual responsible for ensuring that the appropriate operational security posture is maintained for an information system and as such, works in close collaboration with the information system owner. The information system security officer also serves as a principal advisor on all matters, technical and otherwise, involving the security of an information system. The information system security officer has the detailed knowledge and expertise required to manage the security aspects of an information system and, in many organizations, is assigned responsibility for the day-to-day security operations of a system.

OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, Appendix 1 states agencies are to:

- Implement policies and procedures to ensure that all personnel are held accountable for complying with agency-wide information security and privacy requirements and policies.
- Implement security and privacy controls, and verify that they are operating as intended, and continuously monitored and assessed; put procedures in place so that security and privacy controls remain effective over time, and that steps are taken to maintain risk at an acceptable level within organizational risk tolerance.
- Correct deficiencies that are identified through information security and privacy assessments, information system continuous monitoring and privacy continuous monitoring programs, or internal or external audits and reviews, to include OMB reviews.

In order to appropriately manage risk from an organization-wide structure, the Department and FSA CISOs need to hold accountable those individuals responsible for ensuring that persistent IT control deficiencies are remediated and the appropriate security posture is maintained for Department and FSA information systems.

INDEPENDENT AUDITORS' REPORT (Continued)
EXHIBIT A
Significant Deficiencies

Recommendations:

We recommend the Principal Deputy Assistant Secretary, Office of Management:

- 2a. Implement a monitoring process over the personnel security activities to ensure investigations and reinvestigations are prioritized for personnel with sensitive system access within the Department.

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

- 2b. Strengthen and refine the process for holding system owners and information system security officers accountable for remediation of control deficiencies and ensuring that the appropriate security posture is maintained for Department and FSA information systems.

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

Requirement for Referring Delinquent Student Loan Debts to Treasury

In 2014, Federal law³ was amended⁴ to require 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 (i.e. collection through the reduction of future Federal payments). Due to the number of entities and systems involved in handling student loan debts, FSA is not yet capable of meeting this accelerated timeline. Accordingly, as of September 30, 2017, the Department and FSA are not in compliance with the legal requirement for referring 120 day delinquent student loan debts to Treasury.

To meet this requirement, the Department obtained legal clarification of how certain specific requirements of the amended law apply to the Direct Loan Program and other Department programs, improve delinquent debt reporting procedures, increase the frequency of some debt referrals and modify its defaulted loan management system to accommodate this change. The Department is also evaluating the impact of defining defaulted loans earlier on schools' performance reporting and has developed a long-term project plan to incorporate the new referral requirements into various servicer contracts and guaranty agency agreements, so they can initiate the required system programming changes. FSA is also working with the Department in evaluating certain options for other requirements needed to achieve compliance.

Recommendation:

We recommend that the Secretary of Education work with the Federal Student Aid Chief Operating Officer to:

3. Continue to execute the corrective actions as outlined in FSA's project plan to comply with the timing requirement for the referral of delinquent non-tax debts.

³ 31 U.S. Code Section 3716(c)(6)

⁴ Public Law 113-101 (DATA Act) Section 5

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



UNITED STATES DEPARTMENT OF EDUCATION
WASHINGTON, DC 20202

NOV 09 2017

MEMORANDUM

TO: Kathleen S. Tighe
Inspector General

FROM: Tim Soltis *Tim Soltis*
Delegated the Duties of Chief Financial Officer

Jason Gray *Jason Gray*
Chief Information Officer

SUBJECT: DRAFT INDEPENDENT AUDITORS' REPORT
Fiscal Years 2017 and 2016 Financial Statements
U.S. Department of Education
ED-OIG/A17R0001

Please convey the Department's sincere thanks to everyone on your staff who worked diligently on this financial statement audit. We extend our appreciation for the professionalism and commitment by all parties, including the Office of the Inspector General and CliftonLarsonAllen, throughout the audit process.

We have reviewed, and concur and agree with, the draft Independent Auditors' Report. We are pleased to have received an unmodified "clean" audit opinion with no material weaknesses. The Department takes the two significant deficiencies reported, in the areas of controls over modeling activities and information technology controls, very seriously and we are dedicated to resolving the issues identified. We will share the final audit results with responsible senior officials, other interested program managers, and staff who will begin preparing 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.

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 2016 Recommendations	Fiscal Year 2017 Status
CLA Recommended that the Deputy Secretary:	
1a. Perform a comprehensive evaluation of the impact of the Department's modeling on the Department's mission in connection with the development of its enterprise risk management program.	Modified Repeat, see Significant Deficiency
CLA Recommended the Department Chief Financial Officer, in conjunction with the Director, Budget Service:	
1b. Document the Department's process, policies and procedures for the design, development, testing and authorization of new models.	Modified Repeat, see Significant Deficiency
1c. Compile an inventory of the Department's models, and regularly document management's assessment of risks related to each model and how that assessment impacts the Department's level of controls, validation and monitoring over each model.	Modified Repeat, see Significant Deficiency
1d. Document the Department's process, policies, procedures and related controls for the periodic review, validation and approval of the Department's models at the model and program level.	Modified Repeat, see Significant Deficiency
1e. Document the overall review and conclusions drawn related to the evaluation of the results of model performance reviews and validation procedures performed.	Modified Repeat, see Significant Deficiency
CLA Recommended the Director, Budget Service and the Department and FSA Chief Financial Officers:	
1f. Document the Department's process, policies, procedures and related controls for managing the operation and use of approved models.	Modified Repeat, see Significant Deficiency
1g. Design, document and implement a modeling governance structure that specifically and separately addresses the roles and responsibilities for the oversight of critical modeling activities, including model risk assessment, model development, model operation, and model validation activities, as well as defining standards for policies, procedures and internal controls for these activities.	Modified Repeat, see Significant Deficiency
CLA Recommended the Department Chief Financial Officer:	
1h. Ensure the agency's management controls program fully evaluates the Department's modeling activities commensurate with the materiality of the impact of the process to the agency's reporting activities.	Modified Repeat, see Significant Deficiency

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

CLA Recommended the Department CIO:	
2a. Ensure the update, review, approval and dissemination of the Information Assurance/ Cybersecurity Policy and associated guidance is completed in order to comply with NIST standards and OMB guidance.	Closed
2b. Design and implement controls over the handling of Department security and privacy incidents to ensure their resolution is properly documented.	Modified Repeat, see Significant Deficiency
CLA Recommended the Principal Deputy Assistant Secretary, Office of Management:	
2c. Implement a monitoring process over the personnel security activities to ensure investigations and reinvestigations are prioritized for personnel with sensitive system access within the Department.	Modified Repeat, see Significant Deficiency
CLA Recommended the Department CISO work with the FSA CISO to:	
2d. Strengthen and refine the process for holding system owners and information system security officers accountable for remediation of control deficiencies and ensuring that the appropriate security posture is maintained for Department and FSA information systems.	Modified Repeat, see Significant Deficiency
Noncompliance with Laws and Regulations	
3. CLA recommended that the Secretary of Education work with the Federal Student Aid Chief Operating Officer to continue to execute the corrective actions as outlined in FSA's project plan to comply with the timing requirement for the referral of delinquent non-tax debts.	Repeat