Analysis of Systems, Controls, and Legal Compliance

Management Assurances

The Secretary of Education's 2016 Statement of Assurance provided below is the final report produced by the Department's annual assurance process.

STATEMENT OF ASSURANCE
FISCAL YEAR 2016
November 14, 2016

The Department of Education (the Department) management is responsible for meeting the objectives of the *Federal Managers' Financial Integrity Act of 1982* (FMFIA) by establishing, maintaining, evaluating, and reporting on the Department's internal control and financial systems.

In accordance with Section 2 of FMFIA and Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control,* management evaluated the effectiveness of the Department's internal controls to support effective and efficient programmatic operations, reliable reporting, and compliance with applicable laws and regulations.

Section 4 of FMFIA and the *Federal Financial Management Improvement Act of 1996* (FFMIA) require management to ensure the Department's financial management systems provide reliable, consistent disclosure of financial data. In accordance with Appendix D of OMB Circular A-123, management evaluated whether the Department's financial management systems substantially complied with FFMIA requirements. The Department also conducted a separate assessment of the effectiveness of its internal control over financial reporting, including controls designed to prevent, detect, and recover improper payments, in accordance with Appendix A of OMB A-123.

The Department has not identified any material weaknesses in operations, reporting, or compliance with applicable laws and regulations.

Based on the results of the Department's assessments described above, our system of internal controls provides Department management with reasonable assurance that the objectives of sections 2 and 4 of the FMFIA were achieved as of September 30, 2016.

John B. King, Jr.

Introduction

Strong risk management practices and internal control help an entity run its operations efficiently and effectively, report reliable information about its operations and financial position, and comply with applicable laws and regulations. The FMFIA requires federal agencies to establish internal controls that provide reasonable assurance that agency objectives will be achieved. OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* implements FMFIA and defines management's responsibilities for ERM and internal control. The Circular provides guidance to federal managers to improve accountability and effectiveness of federal programs as well as mission support operations through implementation of ERM practices and by establishing, maintaining, and assessing internal control effectiveness. The guidance requires federal agencies to provide reasonable assurance that it has met the three objectives of internal controls:

- *Operations*—Effectiveness and efficiency of operations;
- *Reporting*—Reliability of reporting for internal and external use; and
- *Compliance*—Compliance with applicable laws and regulations.

This section describes the Department's internal control framework, an analysis of the effectiveness of its internal controls, and assurances provided by the Department's leadership that internal controls were in place and working as intended during FY 2016 to meet the three objectives.

Control Framework and Analysis

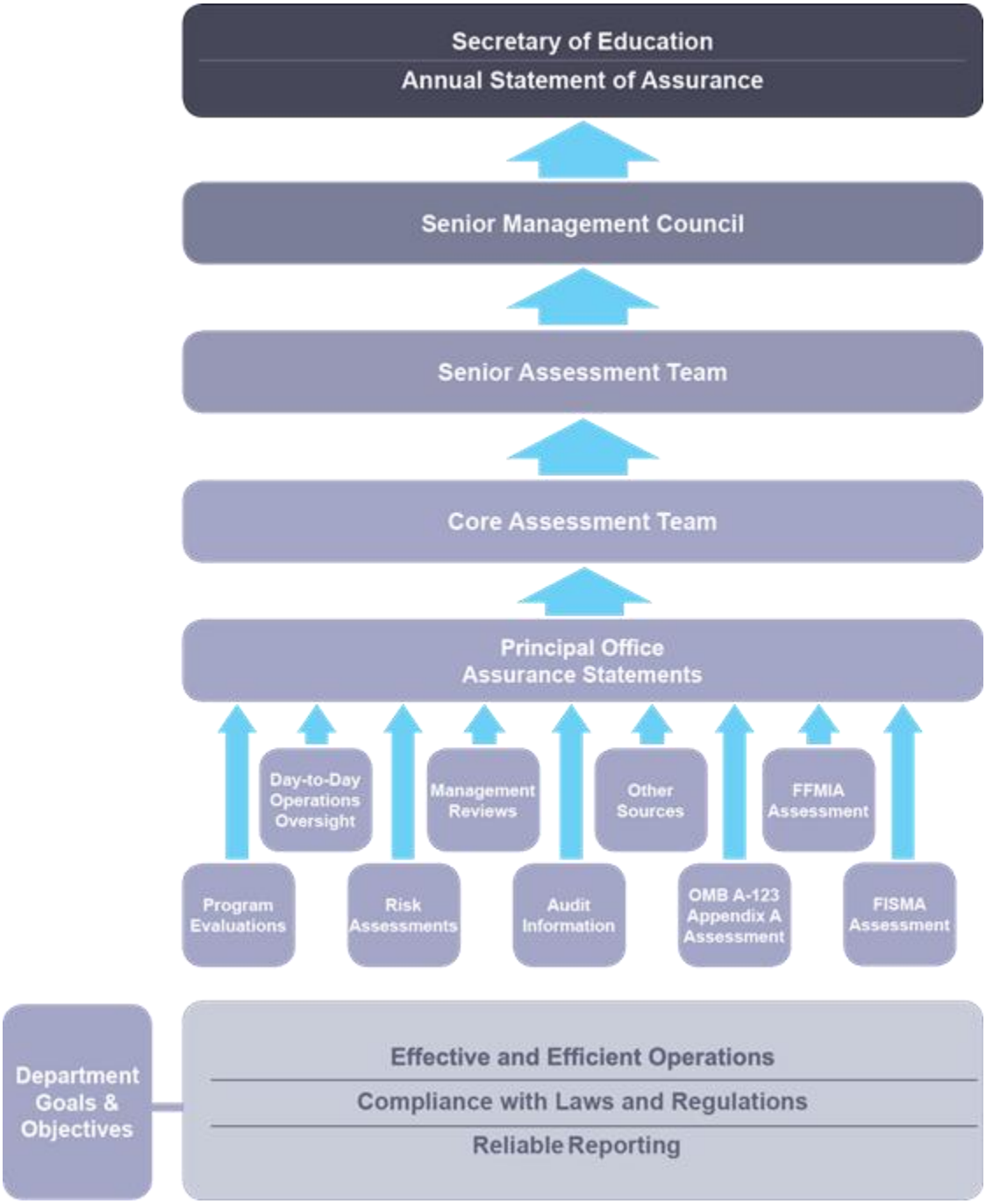
As indicated in the performance management section above, the Department's *Strategic Plan*, including the six FY 2016–17 APGs, sets the foundation for determining the Department's mission goals and objectives. Underpinning the Department's internal control framework are its organizational structure, people, processes, policies and procedures, systems, controls, and data.

Control Framework

The Department's internal control framework helps to ensure that the Department achieves its strategic goals and objectives related to delivering education services effectively and efficiently while complying with all applicable laws and regulations and preparing accurate reports. This includes providing reasonable assurance to Department leadership and external stakeholders that financial data produced by the Department's financial systems are complete, accurate, and reliable enough to support the preparation and fair presentation of financial statements that conform to federal standards, facilitate sound financial decision-making, and provide transparency about how the Department spent federal funds and maintains stewardship over its financial resources.

The Department maintains a comprehensive internal control framework and assurance process as depicted in the following diagram.

Internal Control Framework and Assurance Process



The Office of the Chief Financial Officer (OCFO) manages the assurance process on behalf of Department leadership. The Department established governance over the process, consisting of a Senior Management Council, a Senior Assessment Team (SAT), and a Core Assessment Team (CAT). The Senior Management Council is comprised of senior leaders from across the Department who provide strategic direction and guidance to the SAT and CAT. The SAT and CAT include representatives from OCFO, the Office of the Chief Information Officer (OCIO), student loan and grant-making program offices, Risk Management Service, and other

operational support offices (including the Office of Management). The SAT and CAT provide greater oversight and monitoring of activities related to internal control assessments.

The annual assurance process is the primary mechanism by which the Department implements FMFIA and OMB requirements pertaining to internal control. It requires the head of each principal office to evaluate its respective internal controls and to assert, in a letter to the Chief Financial Officer, that it has reasonable assurance that key internal controls are in place and working as intended or to provide a detailed description of significant deficiencies, material weaknesses, and other matters of nonconformance. In making their assessment, principal office staff consider information such as office managers' personal knowledge of operations, external audit results, internal assessments, and other related material.

OCFO staff work with the principal offices to help them identify potential control deficiencies and consults with the SAT to determine whether they represent significant deficiencies or potential material weaknesses. Any principal office that identifies a significant deficiency or material weakness must prepare a Corrective Action Plan to address the issue. These Corrective Action Plans, in addition to daily operational oversight and management-initiated evaluations, facilitate the correction and monitoring of controls. If potential material weaknesses are identified, they are evaluated by the Senior Management Council to determine if they should be reported on the Department's Statement of Assurance.

Analysis of Controls

Overall, the Department relies on the principal office annual assurances, supported by risk-based internal control evaluations and testing, to provide reasonable assurance that its internal controls are well designed and in place and working as intended. The Department also considers issues identified by external auditors. During FY 2016, the Department revised its annual assurance process to conform to the new requirements contained in the revised U.S. Government Accountability Office publication, *Standards for Internal Control in the Federal Government* (commonly referred to as the "Green Book"). Additionally, the Department overhauled its entity-level assessment to reflect the updated Green Book.

In FY 2016, the Department identified no material control weaknesses related to effective and efficient program operations and no areas of noncompliance with laws and regulations other than those noted in the Internal Control Exceptions section below. Although no material weaknesses were identified, the Department realizes that it has areas of control that need further strengthening, such as those disclosed in this report and the major challenges identified by the Department's OIG in its *OIG FY 2017 Management Challenges* report. The Department continues to demonstrate its commitment to addressing, mitigating, or resolving its identified management challenges, at the level of root cause, to ultimately eradicate systemic and persistent barriers to achieving its mission, and optimal performance.

In accordance with OMB Circular A-123, the Department also conducted an additional assessment of the effectiveness of the Department's internal controls over financial reporting and compliance with key financial management laws and regulations as described below.

Internal Control over Financial Reporting

The Department maintains strong internal controls to identify, document, and assess internal control over financial reporting, which includes:

- comprehensive process documentation for the Department's significant business processes and subprocesses,
- maintenance of a control catalogue composed of 1,716 key financial and operational controls that align to the business processes[6] (the Department monitors 312 key controls and FSA monitors 1,404 key controls [243 entity-level controls, 850 servicer controls, 311 FSA controls]),
- technical assistance provided to principal offices to help them understand and assess key financial controls,
- a risk-based testing strategy, and
- a process to develop corrective action plans when control deficiencies are found and to track progress against those plans.

During FY 2016, the Department tested 150 key financial controls. Although some weaknesses were detected in the design and effectiveness of controls, the Department did not identify any material weaknesses. Corrective actions have been initiated for the deficiencies identified.

Furthermore, to ensure data accuracy and strengthen internal controls, the Department migrated 20 of its manual reconciliations to an automated reconciliations platform. The Department has undertaken a broader FM segment modernization plan and has identified further manual reconciliations to be automated in the future.

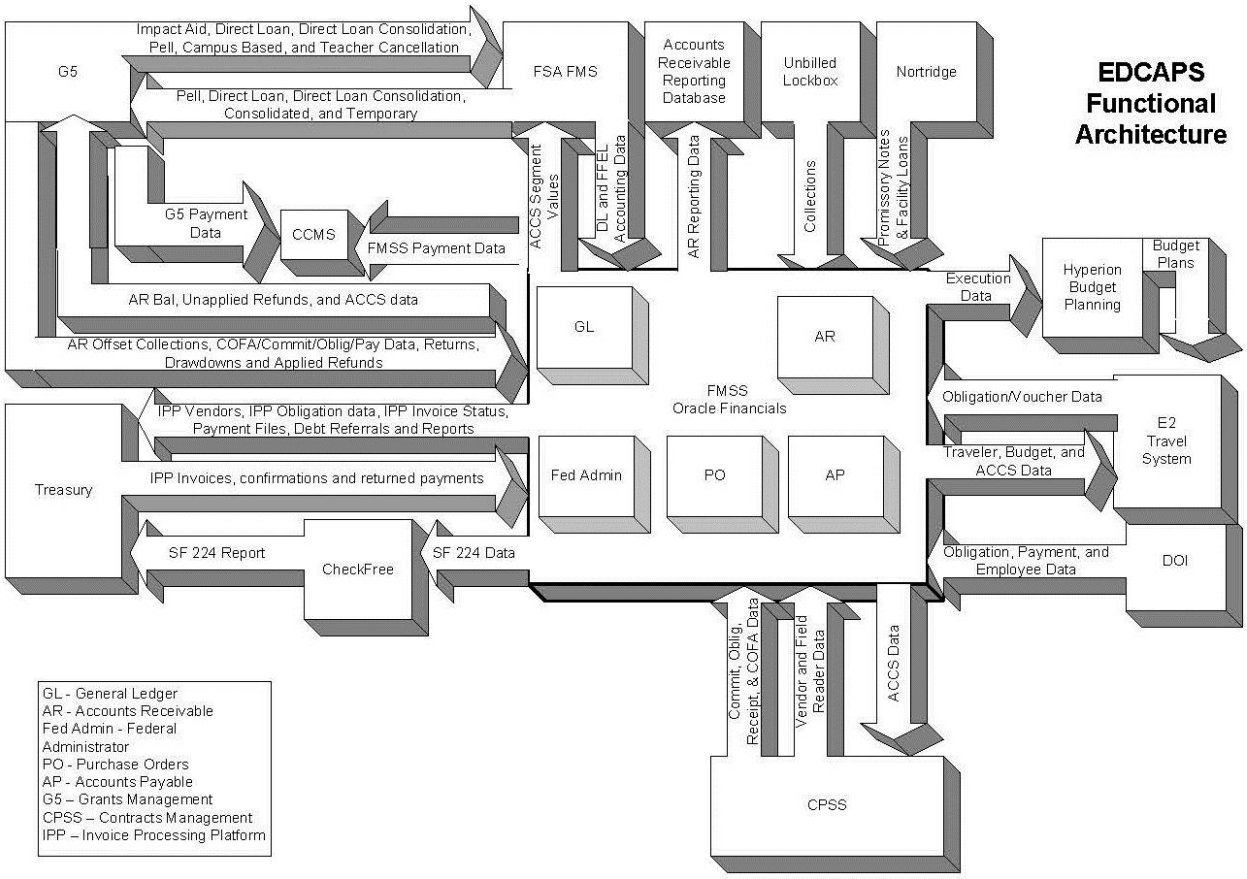
Internal Control over Financial Management Systems

The FFMIA requires management to ensure that the Department's financial management systems consistently provide reliable data that comply with federal financial management system requirements, applicable federal accounting standards, and the U.S. Standard General Ledger at the transaction level. Appendix D to OMB Circular A-123, Compliance with the Federal Financial Management Improvement Act of 1996, and OMB Circular A-130, *Managing Federal Information as a Strategic Resource,* provide specific guidance to agency managers when assessing conformance to FFMIA requirements.

The Department's core financial systems are under the umbrella of the Education Central Automated Processing System (EDCAPS), serving approximately 8,800 Departmental internal users in Washington, D.C., and 10 regional offices throughout the United States, as well as 39,600 external users. EDCAPS is composed of five main linked components:

- Financial Management Support System (FMSS),
- Contracts and Purchasing Support System (CPSS),
- Grants Management System (G5),
- E2 Travel System, and
- Hyperion Budget Planning.

[6] These figures include FSA.



The Department designated the FMSS as a mission-critical system that provides core financial management services, and focused its system strategy on the following areas during FY 2016:

- managing and implementing cross-validation rules throughout the fiscal year to prevent invalid accounting transactions from being processed,
- developing an interface solution with FSA to eliminate the manual collections processing of funds returned to the Department for Perkins Loan Program,
- transmitting the Department's spending data related to contracts, grants, loans, and other financial assistance awards for the USASpending.gov initiative as part of the *Federal Funding Accountability and Transparency Act of 2006,*
- meeting required timelines for a successful *Digital Accountability and Transparency Act of 2014* (DATA Act) implementation, and
- establishing transaction assurance reports for validating the condition of data processed through external interface files.

In FY 2017, EDCAPS will continue to provide customer service and improve security of its systems by completing the Department's compliance with Homeland Security Presidential Directive (HSPD-12) user access requirements. The Department is also working to implement interface enhancement between the Invoice Processing Platform and FMSS to automate the receipt creation process, the Purchase Order balances and invoices matching process, and the invoice approval process in FMSS.

The Department's financial management systems are designed to support effective internal control and produce accurate, reliable, and timely financial data and information. Based on self-assessments, system-level general controls tests, and the results of external audits, the Department has not identified any material weaknesses in controls over systems. The Department has also determined that its financial management systems substantially comply with FFMIA requirements. However, as noted below in the Internal Control Exceptions section, the Department continues to address issues and improve its controls over systems.

Federal Information Security Modernization Act of 2014

The *Federal Information Security Modernization Act of 2014* (FISMA) requires federal agencies to develop, document, and implement an agencywide program to provide security for the information and information systems that support the operations and assets of the agency and ensure the confidentiality, integrity, and availability of system-related information.

The Department's and FSA's information security programs completed a number of significant activities in FY 2016 to improve cybersecurity capabilities and functions, some of which included:

- With the issuance by OMB of the federal government's Cybersecurity Strategy and Implementation Plan (CSIP), the Department focused many of its efforts in FY 2016 to address the recommendations and actions highlighted in the CSIP in order to resolve any cybersecurity gaps and emerging priorities that were noted across the government. The CSIP required the Department to prioritize the identification and protection of high-value information and assets. The Department completed this action, which will enable the Department to better understand the potential impact from a cyber incident, and helps to ensure that robust physical and cybersecurity protections are in place for our high-value assets (HVAs).
- The Department continued to enhance the capabilities of the Department's Security Operations Centers (SOCs). The Department has fully deployed the Einstein capabilities in order to enhance our ability to detect cyber vulnerabilities and protect against cyber threats. The Department has also continued to strengthen its partnership with DHS for the project planning that will accelerate the deployment of Continuous Diagnostics and Mitigation (CDM) capabilities. This will further enhance capabilities that the Department initiated in 2016 to implement network access control (NAC) and data loss prevention (DLP) solutions. The CDM solution will also enable the Department to enhance our configuration management capabilities.
- The Department continued its progress of implementing and enforcing the use of multifactor authentication for all federal employees, contractors, and other authorized users. The Department and FSA focused on increasing the issuance of Personal Identity Verification (PIV) and PIV-I two-factor authentication cards to privileged users to meet OMB requirements.
- The Department made significant strides in its identification, tracking, and remediation of unsupported software across the enterprise.
- The Department achieved all targets in the completion of required annual cybersecurity training courses, and also successfully completed a number of phishing exercises. Of note, 100 percent of Department users completed the annual computer security and privacy awareness training course. The Department strictly enforced compliance with annual

security and privacy awareness training requirements, and disabled network accounts for noncompliant users.

- There has also been an increased Departmental focus on data security at institutions of higher education (IHEs). FSA issued a new "Dear Colleague Letter" to IHEs that receive financial aid stressing the need to comply with the *Gramm-Leach-Bliley-Act* (GLBA) standards and announcing that these standards would now be included in future reviews to be conducted by the Department. The Department recognizes that it is vital to focus on cybersecurity at these IHEs as they connect to FSA systems and access FSA data. It is noteworthy that the Department has successfully implemented two-factor authentication for all external users of the G5 system, which is a customer-facing grants management system. The Department has also engaged the General Services Administration to investigate the use of Login.gov for two-factor authentication to other Department citizen-facing information systems.

As a result of the Department implementing a comprehensive set of activities to strengthen the overall cybersecurity of the Department's networks, systems, and data, significant improvements in its information security program were highlighted by the Department completing actions to close 25 of the 26 recommendations to address the 16 findings made by the OIG in its FY 2015 annual FISMA audit. For the FY 2016 annual FISMA audit, the OIG is only reporting 15 recommendations to address 11 findings, which reflects a noteworthy drop in the total number of findings and recommendations from the previous reporting year.

The OIG FISMA Audit objective was to conduct annual independent evaluations and tests to determine the effectiveness of the information security program policies, procedures, and practices of the Department. Unfortunately, the OIG was provided revised guidance in the last week of the fiscal year for how to score and assess the effectiveness and maturity levels achieved in each of the major parts of the Department's information security program. This late issuance of the guidance left the Department unable to prioritize or allot resources early in the fiscal year to better address some of the specific criteria that were part of the new OIG scoring methodology. The FY 2016 OIG FISMA reporting metrics are organized around the five security functions outlined in the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. The overall results of the OIG audit work for FY 2016 determined that the Department's implementation of two of the five Cybersecurity Framework security functions were assessed to be effective and were rated to be at the highest maturity level. The two Department security functions that were determined to be effective are the security elements of Identify and Recover. The OIG also assessed that the Department needed to continue to make improvements in order to achieve effective maturity level ratings in the Cybersecurity Framework security functions of Protect, Detect, and Respond.

The FY 2016 Financial Statement Audit report contained three new recommendations for the Chief Information Officer's attention:

- 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;
- Design and implement controls over the handling of Department security and privacy incidents to ensure their resolution is properly documented; and

- 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.

The following recommendations were noted as "Repeat Findings" in the audit report:

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

The Department Chief Information Officer concurs with the recommendations and will be developing the required corrective action plans to address them.

Internal Control over Payments

The Department's FY 2016 Statement of Budgetary Resources reports $285 billion in total outlays, consisting of appropriated budgetary resources of $88 billion and non-budgetary credit program funding of $197 billion. The Department developed robust internal controls to ensure payment integrity and to prevent, detect, and recover improper payments. Key controls related to payment integrity include:

- preaward risk assessments,
- use of independent data sources (such as IRS data retrieval) to ensure accurate award amounts,
- automated system controls to detect and prevent payment errors, and
- award and payment monitoring.

Additionally, the Department must rely on controls established by fund recipients who make payments on behalf of the Department. These controls are outside of the Department's operational authority and present higher risks, as evidenced by the OIG work identifying instances of questioned costs and restitution payments.

As described below, in FY 2016, the Department determined that its Pell Grant and Direct Loan programs were susceptible to significant improper payments risk. A detailed description of the Department's controls over improper payments related to these two programs is presented in the Other Information section of this report.

In addition, the Department launched Phase I of the Payment Integrity Workgroup in FY 2016 to catalog internal controls around payment integrity to ensure proper payments. Starting in late FY 2016, Phase II of the project is in process to further define and demonstrate payment integrity. The workgroup plans to work collaboratively with process owners to validate internal control measures, develop corrective action plans, address gaps, and ensure the accuracy of the specific controls. The desired outcome of this effort is to minimize improper payments,

improve risk assessment and response, develop more efficiency in the process, and increase positive assurance submissions.

Internal Control Exceptions

The Department identified two instances of noncompliance with laws and regulations in FY 2016. Additionally, reviews and assessments conducted pursuant to information technology-related laws and regulations identified challenges still facing the Department.

Improper Payments Information Act of 2002

The *Improper Payments Information Act of 2002*, Pub. L. 107-300, 116 Stat. 2350, as amended by the *Improper Payments Elimination and Recovery Act of 2010* (IPERA), Pub. L. 111-204, 124 Stat. 2224, and the *Improper Payments Elimination and Recovery Improvement Act of 2012* (IPERIA), Pub. L. 112-248, 126 Stat. 2390, requires federal agencies to annually report improper payments in programs susceptible to significant improper payments. IPERA also requires agency Inspectors General to review agency improper payment reporting in the AFR and accompanying materials, and to determine whether the agency has met six compliance requirements.

OIG audits of the Department's IPERA compliance for FY 2015 and FY 2014 found that the Department was not compliant, because estimated improper payments for the Direct Loan program those years did not meet the annual reduction target published in the prior year AFR. The complete OIG reports are available for review at the OIG website. A detailed description of the findings and corrective actions related to this issue of noncompliance is presented in the Other Information section of this report.

We anticipate that the 2016 OIG audit will again find that, as of September 30, 2016, the Department was not compliant with IPERA because the FY 2016 improper payment rates did not meet the annual reduction targets for the Direct Loan or Pell Grant programs published last year.

This determination of noncompliance with the IPERA does not represent a material weakness in the Department's internal controls.

Debt Collection Improvement Act of 1996

The *Debt Collection Improvement Act of 1996* (DCIA), Pub. L. 104-134, 110 Stat. 1321-358, was enacted into law as part of the *Omnibus Consolidated Rescissions and Appropriations Act of 1996,* Pub. L. 104-134, 110 Stat. 1321. The primary purpose of the DCIA is to increase the collection of nontax debts owed to the federal government. Additionally, the DATA Act, Pub. L. 113-101, 128 Stat. 1146, amended Section 3716(c)(6) of the DCIA to require referral of delinquent debt to Treasury's Offset Program within 120 days.

Due to unique program requirements of HEA, the Department requested guidance from Treasury's Bureau of Fiscal Service, Office of General Counsel for the application of this revised DCIA requirement to Title IV debt. Treasury provided its interpretation of this requirement for Title IV debt in July 2015. As of September 30, 2016, the Department and FSA were not in compliance with the new 120-day referral requirement in 31 U.S.C. Section 3716(c)(6) because FSA had not yet revised its loan servicing systems, procedures, and internal processes in response to this interpretation. During FY 2016, FSA did identify policy changes required to work towards achieving compliance. As of the end of FY 2016, FSA is vetting these policy

changes and expects to begin a multiple-year implementation in FY 2017. This area of noncompliance is noted in the independent auditors' report, exhibit B.

This determination of noncompliance with the DCIA does not represent a material weakness in the Department's internal controls.