

ANALYSIS OF SYSTEMS, CONTROLS, AND LEGAL COMPLIANCE

MANAGEMENT ASSURANCES

The Secretary of Education's 2017 Statement of Assurance provided below is the final report produced by the Department's annual assurance process. Although the Department has not identified any material weaknesses, it acknowledges that there are significant weaknesses and management challenges to be addressed that are identified elsewhere in this report.

STATEMENT OF ASSURANCE FISCAL YEAR 2017 November 13, 2017

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 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 Circular 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, 2017.


Betsy DeVos

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.

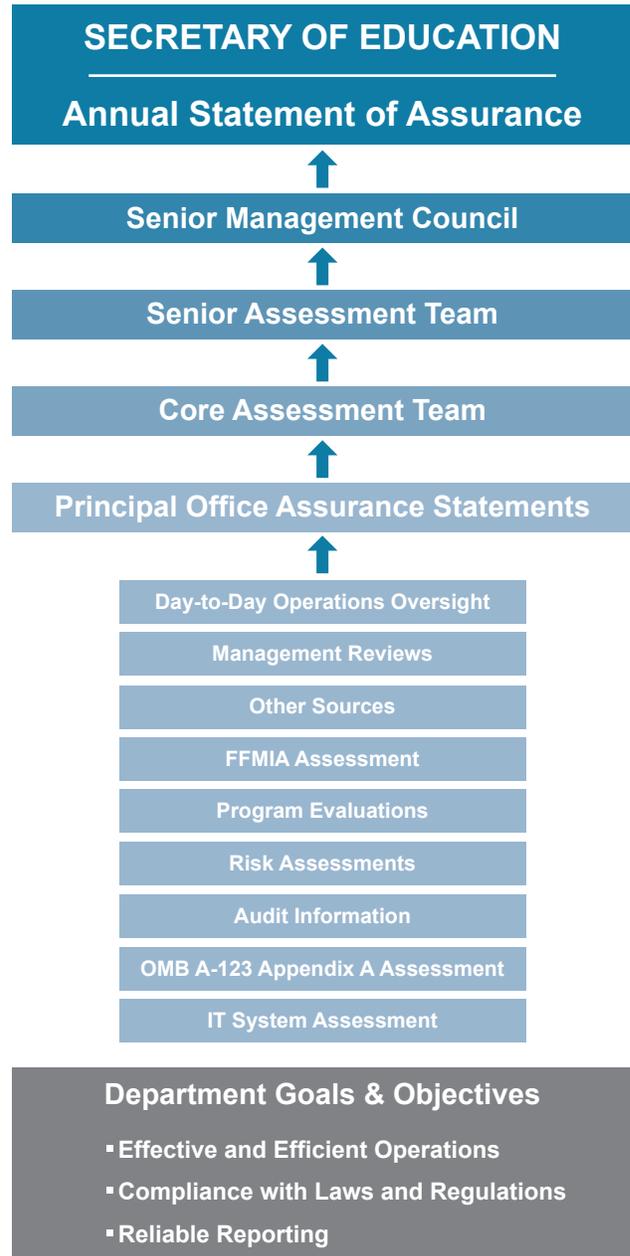
This section describes the Department's internal control framework, an analysis of the effectiveness of its internal controls, and assurances provided by the Department's leadership that internal controls were in place and working as intended during FY 2017 to meet the three objectives.

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 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.

Figure 12. 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. It is the primary governance structure for internal control and provides oversight to ensure management accountability for effective controls across the Department. 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 this assessment, the head of the principal office considers 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 consult 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"). In FY 2017, the Department further revised the process to conform to the revised OMB Circular A-123 issued on July 15, 2016.

In FY 2017, the Department identified no material control weaknesses related to effective, 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 2018 Management Challenges report**. The Department continues to demonstrate its commitment to addressing, mitigating, or resolving its identified management challenges.

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 comprised of 3,631 key financial, operational, and IT controls that align to the business processes (the Department documents 312 key controls and FSA documents 3,319 key controls [1,411 Business Process and Entity-Level controls and 1,908 IT controls]),¹
- 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 2017, the Department tested 84 key financial controls. Although some control deficiencies were detected in the design and effectiveness of controls, the Department did not identify any significant deficiencies or material weaknesses. Corrective actions have been initiated for the deficiencies identified.

In FY 2017, FSA tested 2,810 key controls: 1,342 Business Process and Entity-Level controls and 1,468 IT controls. FSA assessed that 96 percent of the controls tested are designed and operating effectively. The other 4 percent are immaterial deficiencies for which FSA has established or is establishing corrective actions. FSA will continue to repeat this assessment process on a regular basis, constantly looking for opportunities to improve operations.

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.

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 2017:

- Managing and implementing cross-validation rules throughout the fiscal year to prevent invalid accounting transactions from being processed,
- 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*,
- Transmitting the Department's spending data related to contracts, grants, loans, and other financial assistance awards for the *Digital Accountability and Transparency Act of 2014* (DATA Act) implementation, and

¹ These figures include FSA.

- Initiating the upgrade of the FMSS Oracle E-Business Suite application to Oracle R12, to ensure continued vendor support, improved security, improved infrastructure and enhanced functionality.

In FY 2018, EDCAPS will continue to provide customer service and improve security of its systems by completing the Department's implementation of Oracle E-Business Suite R12. In doing so, the Department will be current and ready to provide a more secure and better integrated financial management application.

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 internal and 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 agency wide 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 and FY 2017 to improve cybersecurity capabilities and functions, some of which included:

- In March 2017, the Office of the Chief Information Officer (OCIO) initiated an Information Technology (IT) Systems Assessment process, designed to improve management of the Department's IT systems inventory by:
 - Reexamining/revising the IT systems baseline for both FISMA reportable and non-FISMA reportable IT systems,
 - Enhancing governance and security posture of the Department's IT systems portfolio, informing strategy to address externally hosted systems,
 - Establishing long/short term corrective action plans to address findings, and
 - Rationalizing the IT systems portfolio and inventory.
- The IT Systems Assessment process began with examining the 19 High Value Asset (HVA) systems within the Department. As of September 2017, the OCIO team had completed assessments for all 19 HVA systems.
- With the issuance by OMB of the federal government's Cybersecurity Strategy and Implementation Plan (CSIP), the Department focused many of its efforts 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 and re-validated its list of HVAs in January 2017, 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. The Department completed development of its Cybersecurity Strategy and Implementation Plan (ED-CSIP) in February 2017, which includes the cybersecurity initiatives and activities that demonstrate how the Department is implementing the Cybersecurity Framework functions of Identify, Protect, Detect, Respond, and Recover.

- 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 the Department of Homeland Security 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 and data loss prevention (DLP) solutions. The DLP capability has been activated for the Department's primary network and is effectively detecting and preventing any inadvertent attempts by staff to send social security numbers via e-mail. 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) cards to privileged users to meet OMB requirements. The Department has consistently reported each quarter achieving the Cross Agency Priority target requiring our users to be technically enforced to use their PIV cards when logging on to the network.
- The Department made significant strides in its identification, tracking, and remediation of unsupported software across the enterprise.
- 100 percent of Department users completed the annual computer security and privacy awareness training course in FY 2017. 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* 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 and we have signed a memorandum of understanding to implement a pilot for 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, the Department completed actions to close 10 of the 15 recommendations to address the 11 findings made by the OIG in its FY 2016 annual FISMA audit. For the FY 2017 annual FISMA audit, the OIG is reporting 37 recommendations covering the seven FISMA metrics domains.

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 and Federal Student Aid (FSA). The FY 2017 OIG FISMA reporting metrics were organized around the five security functions outlined in the National Institute of Standards and Technology's "Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover." The FY 2017 maturity model was more comprehensive and attributes were assessed differently than the previous year's maturity model indicator scoring. As a result, certain functions were assessed at a lower level, and the OIG found the Department and FSA were not effective in all five security functions.

INTERNAL CONTROL EXCEPTIONS

The Department identified two instances of noncompliance with laws and regulations in FY 2017. 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* (IPIA), **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**, require federal agencies to annually report improper payments for programs that are deemed susceptible to significant improper payments. IPERA also requires each agency's Office of Inspector General (OIG) to review the agency's improper payment reporting in its AFR and accompanying materials, and to determine whether the agency has met six compliance requirements.

In its annual improper payment compliance audit for FY 2016, the OIG concluded that the Department was not compliant with IPERA because it did not meet two of IPERA's six compliance requirements. The Department reported improper payment rates for the Direct Loan and Pell Grant (Pell) programs that did not meet the FY 2016 reduction targets and the Department's risk assessments for its grant programs managed by offices other than Federal Student Aid (FSA) and contracting activities managed by FSA did not conform to applicable guidance.

This determination of noncompliance with 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, 2017, 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 2017, FSA initiated the change management process for its default loan servicer to refer eligible debts to the Treasury Offset Program sooner, developed DCIA compliant referral exclusions, and continued to identify policy changes required to work towards achieving compliance. 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.

This page intentionally left blank.