ANALYSIS OF SYSTEMS, CONTROLS, AND LEGAL COMPLIANCE

MANAGEMENT ASSURANCES

The Secretary of Education’s 2019 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, the independent auditor identified a material weakness and significant deficiencies in the auditors’ report, and the Office of Inspector General identified management challenges in the Office of Inspector General’s Management and Performance Challenges For Fiscal Year 2020 report.

STATEMENT OF ASSURANCE
FISCAL YEAR 2019
November 15, 2019

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, 2019.

Betsy DeVos

Betsy DeVos

INTRODUCTION

Strong risk management practices and internal controls 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:

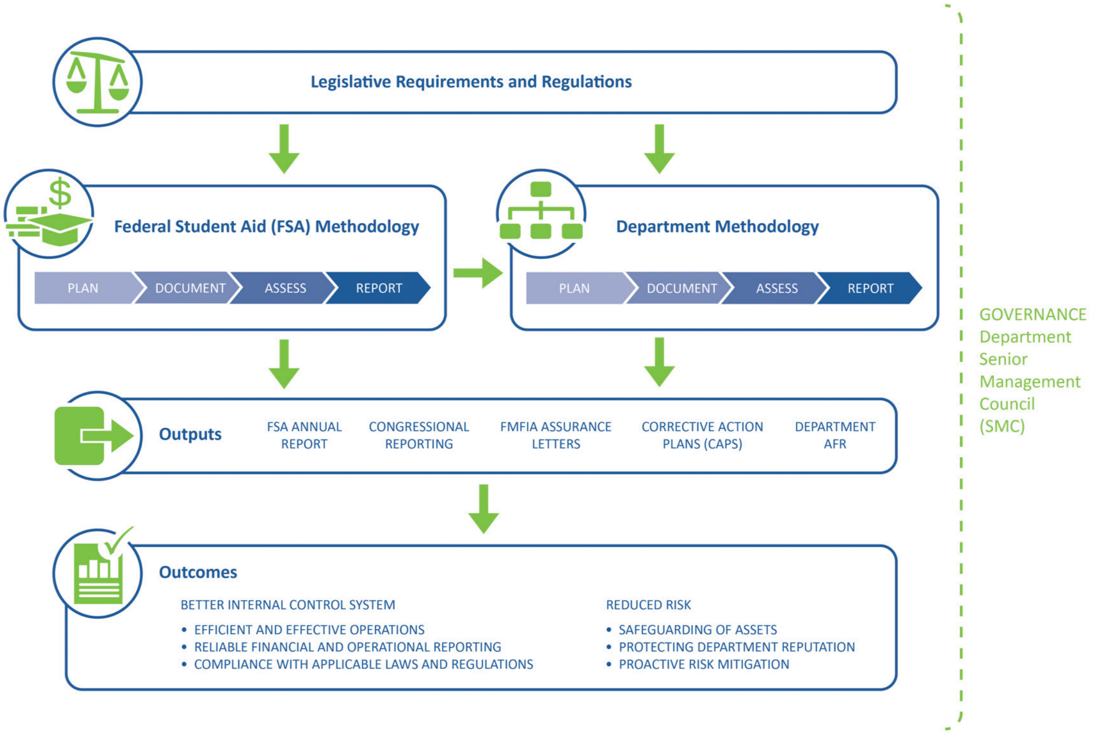
- *Operations*—Effectiveness and efficiency of operations;
- *Reporting*—Reliability of reporting for internal and external use; and
- *Compliance*—Compliance with applicable laws and regulations.

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 2019 to meet the three objectives.

Internal 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, complies with applicable laws and regulations, and prepares accurate reports. The Department maintains a comprehensive internal control framework and assurance process as depicted in the following diagram.

Figure 12. Department of Education Internal Control Framework


Legislative Requirements and Regulations
Federal Student Aid (FSA) Methodology
PLAN
DOCUMENT
ASSESS
REPORT
Department Methodology
PLAN
DOCUMENT
ASSESS
REPORT
Outputs
FSA ANNUAL REPORT
CONGRESSIONAL REPORTING
FMFIA ASSURANCE LETTERS
CORRECTIVE ACTION PLANS (CAPS)
DEPARTMENT AFR
Outcomes
BETTER INTERNAL CONTROL SYSTEM
• EFFICIENT AND EFFECTIVE OPERATIONS
• RELIABLE FINANCIAL AND OPERATIONAL REPORTING
• COMPLIANCE WITH APPLICABLE LAWS AND REGULATIONS
REDUCED RISK
• SAFEGUARDING OF ASSETS
• PROTECTING DEPARTMENT REPUTATION
• PROACTIVE RISK MITIGATION
GOVERNANCE
Department
Senior
Management
Council
(SMC)

The Department has a renewed focus on streamlining and coordinating internal control activities to ensure efficiency of operations, recognizing the connection points across areas, and enabling transparency of information across the Department. This framework enables increased visibility across compliance processes to allow for greater oversight and more informed monitoring of activities related to internal controls and risk management by all offices and governance bodies, including the Department's Senior Management Council. This framework also allows for the Department to obtain the outcomes of a better control system and a reduced risk landscape. Furthermore, this streamlined approach helps the Department provide reasonable assurance to internal and external stakeholders that the data produced by the Department is complete, accurate and reliable, that internal controls are in place and working as intended, and operations are efficient and effective.

ANALYSIS OF CONTROLS

Overall, the Department relies on annual assurances provided by the heads of its principal offices, supported by risk-based internal control evaluations and testing, and annual internal control training for all employees, to provide reasonable assurance that its internal controls are well designed and in place and working as intended. The Department's annual assurance process conforms to the 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") and OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control.*

In FY 2019, the Department identified no material weaknesses related to effective, efficient program operations and no areas of noncompliance with laws and regulations other than those noted in the Analysis of Legal Compliance 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, the Independent Auditors' Report, and the major challenges identified by the Department's OIG in its OIG FY 2020 Management Challenges report. As an example, the creation of the Office of Grants Administration (OGA) in FY 2019 helped strengthen internal control in grants management at the Department. OGA provides guidance and oversight of the Department's discretionary and formula grants policy, training, audit resolution, and indirect cost negotiation.

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

Internal Control over Reporting

The Department maintains processes and procedures to identify, document, and assess internal control over reporting, which includes:

- Comprehensive process documentation for the Department's significant business processes and subprocesses;
- Maintenance of an extensive library of key financial, operations, and Information Technology (IT) controls;
- Technical assistance provided to principal offices to help them understand and monitor key controls;
- A Data Quality Plan to improve reporting controls and data quality;
- A risk-based control testing strategy; and
- A process to develop corrective action plans when internal control deficiencies are found and to track progress against those plans.

The FY 2019 internal controls assessment detected some deficiencies, but none that would rise to the level of material weakness. Corrective actions have been initiated for the deficiencies identified.

ANALYSIS OF 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 vision for its financial management systems is to provide objective financial information to stakeholders to support data-driven decision-making, promote sound financial management, and to enhance financial reporting and compliance activities. The Department's core financial applications have been brought together under common management control under the umbrella of Education Central Automated Processing System (EDCAPS). EDCAPS is a suite of financial applications (subsystems), including commercial off-the-shelf and custom code and interfaces that encompass the Department's core financial management processes. Specifically, EDCAPS provides the following functions:

- General ledger - Preparation of financial statements and reconciliation of general ledger balances with subsystems maintained in program areas and Treasury;
- Funds management - Budget formulation, budget execution, and funds control;
- Grants pre- and post-award processing, including grant payment processing;
- Contract pre- and post-award processing;
- Receivable management;
- Cost management;
- Recipient management; and
- Administrative processes (e.g., purchasing, travel, and miscellaneous payments).

EDCAPS is composed of five main integrated components:

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

EDCAPS is serving approximately 5,300 Departmental internal users in Washington, D.C. and 10 regional offices throughout the United States. EDCAPS is serving approximately 37,900 external users, mostly users of G5. In FY 2019, the Department conducted an annual risk assessment of EDCAPS and tested 82 IT security controls out of a baseline of 630 IT security controls. No significant deficiencies or material weaknesses were identified.

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 2019:

- 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 entire Department's payments through the Department of Treasury Secure Payment System; and
- Transmitting the Department's spending data related to contracts, grants, loans, and other financial assistance awards for the DATA Act implementation.

Budget constraints limit funding for innovation and modernization, requiring the Department to direct available funding and resources to support the steady state of existing investments. However, in November 2018, the Department completed 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. The Department's primary objective is to stabilize Oracle R12, which is the Department's core financial system (FMSS), and any implications of the infrastructure upon which it is hosted (Portfolio of Integrated, Value Oriented Technologies – Hosting), with the goal of achieving a future state where core financial systems and related business systems, support services, and infrastructure have migrated to the maximum extent possible to standard applications and shared services.

The FMSS Oracle E-Business Suite application is behind the Department firewall and not external-facing. FMSS includes the following interfaces to multiple applications which are either not part of the Oracle suite of applications in the Enterprise Resource Planning or are outside the financial management segment:

- Hyperion Budget Planning module – currently only the license fees are included in FMSS investment;
- ED Facilities Loan System (Nortridge) – currently only the license fees are included in FMSS investment;
- The Invoice Processing Platform;
- FSA-FMS financial data;
- Lockbox;
- Department of the Treasury systems; and
- Department of Interior systems.

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 these systems. The Department has also determined that its financial management systems substantially comply with FFMIA requirements. However, as noted below in the Analysis of Legal Compliance section, the Department continues to address issues and improve its controls over systems.

ANALYSIS OF LEGAL COMPLIANCE

The Department is committed to maintaining compliance with applicable laws and regulations. Below are some examples:

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 the *Higher Education Act of 1965* (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. Per Treasury General Counsel's July 2015 legal determination, compliance for Title IV debt requires that the Title IV debt be: 1) in technical default (i.e., 271 days delinquent per Title IV aging) and 2) a receivable of the federal government. Therefore, the DCIA Treasury Offset Program referral requirement for Title IV debt owned by FSA at the time of delinquency is 271 days delinquent and for debt acquired via a FFEL guarantee default claim or default Perkins Loan assignment is 120 days delinquent (per DCIA aging which begins upon acceptance of a defaulted debt). As of September 30, 2019, the Department and FSA were not in compliance with the DCIA Treasury Offset Program referral requirement for Title IV debt as interpreted by Treasury because FSA had not yet revised its loan servicing systems, procedures, and internal processes in response to this interpretation. During FY 2019, FSA continued to implement changes to its default loan servicing system and business process for referring eligible debts to the Treasury Offset Program sooner. In addition, FSA provided guidance to the Guaranty Agencies that will facilitate sending debts to Treasury sooner. FSA will build DCIA requirements into the NextGen FSA servicing platform. This area of noncompliance is noted in the independent auditor's report, exhibit C.

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

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 several significant activities in FY 2019 to improve cybersecurity capabilities and functions, some of which included:

- OCIO publishes monthly Cyber Security Framework (CSF) Risk Scorecards as part of the Department's Information Security Continuous Monitoring (ISCM) efforts to identify cybersecurity risks, issues, and opportunities for improvements in our cybersecurity protections. The CSF Risk Scorecard provides a detailed analysis tool for Authorizing Officials, Information System Owners (ISOs), and Information System Security Officers (ISSOs) to prioritize and mitigate risks to the Department's information systems. The CSF Risk Scorecard was enhanced during FY 2019 to allow for automated risk scoring, improved accessibility, more granular and user-friendly data filtering capabilities, and enhanced data modeling. The continued use of the CSF Risk Scorecards enabled the Department to prioritize resources to resolve identified vulnerabilities. This prioritization led to the closure of all past due Plan of Actions & Milestones (POA&Ms) for the Department's High Value Assets. Overall, the Department has reduced total POA&Ms by more than 83% and delayed POA&Ms by 95%.

- Annually, all Department users are required to complete multiple computer security and privacy awareness training courses. The Department strictly enforces compliance with the training requirements and disables network accounts for users who fail to complete required trainings by established deadlines. In FY 2019, the Department employed increasingly complex phishing scenarios and established administrative mechanisms to enhance user education and awareness of the risks associated with their susceptibility to cyber threats. The Department experienced increases in the Department of Education Security Operations Center (EDSOC) reporting rates for phishing exercises.

- OCIO revised the Department's cybersecurity policy and guidance.

- The updated policy framework was revised to include a new review and approval process for cybersecurity policies, standards, and instructions. This process includes automated workflows, pre-defined review timelines, and delegated approval authorities which will improve the Department's agility in providing critical time-sensitive guidance and requirements to Department system stakeholders.

- OCIO developed and published Departmental Guidance/Standard Operating Procedures (SOPs) to assist the Department points of contact (POCs) with finalizing the quarterly and annual FISMA reporting requirements. OCIO developed and published both an internal OCIO review procedure and external guidance document for use by POCs. These documents collectively outline a new process for ensuring that the POCs are reporting accurately, and that reports are reviewed, approved and submitted in accordance with established timelines.

- OCIO identified and documented all FedRAMP Cloud Service Providers (CSPs) currently leveraged by the Department and established a Cloud Service Portfolio of CSPs that have been authorized for use. The activities enabled the Department to streamline the processes associated with selecting, assessing and authorizing CSPs. This prevents the acquisition of potentially redundant or duplicative cloud services and streamlines the process of obtaining new service offerings or migrating existing systems to cloud services.

- The Department has begun creating an externally hosted provider inventory to facilitate documentation of externally hosted providers currently leveraged by Department systems, similar to the efforts to strengthen security controls for CSPs. This inventory enables documentation of the various externally hosted providers being leveraged and allows for the imposition of security control inheritance for Department systems that are hosted externally.

- FSA completed a system Personally Identifiable Information (PII) risk assessment process to determine and evaluate how PII is identified, minimized, categorized, and safeguarded, and how incident responses are provided for PII security incidents. FSA also implemented a PII dashboard to report PII risk and developed mitigation strategies for PII risks identified through the initial risk assessment process.

- The Department conducted quarterly Contingency Plan Testing (CPT) and Incident Response Plan (IRP) tabletop exercises. This service allowed Department ISOs and ISSOs to complete the required annual contingency and incident response testing through a professionally facilitated workshop which exposes system stakeholders to new requirements, test scenarios and Department resources. As a result of this effort, CPT and IRP testing compliance across the Department increased from 63 percent to 92 percent.