ANALYSIS OF SYSTEMS, CONTROLS, AND LEGAL COMPLIANCE

MANAGEMENT ASSURANCES

The Secretary of the Department of Education's Fiscal Year 2020 Statement of Assurance provided below is the final report produced by the Department's annual assurance process.

STATEMENT OF ASSURANCE
FISCAL YEAR 2020

November 16, 2020

The Department of Education's (the Department) management is responsible for managing risks and maintaining effective internal control to meet the objectives of the *Federal Managers' Financial Integrity Act of 1982* (FMFIA).

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 assessed risk and 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. Management evaluated the Department's financial management systems for substantial compliance with FFMIA requirements. The Department also conducted a separate assessment of the effectiveness of its internal control over reporting with consideration of its Data Quality Plan in accordance with Appendix A of OMB Circular A-123.

With the exception of a material weakness in financial reporting reported in the Independent Auditors' Report, 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 the Department's management with reasonable assurance that the objectives of Sections 2 and 4 of the FMFIA were achieved as of September 30, 2020.

Betsy DeVos

Betsy DeVos

INTRODUCTION

Strong risk management practices and internal control help the Department 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 (ERM) 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 control:

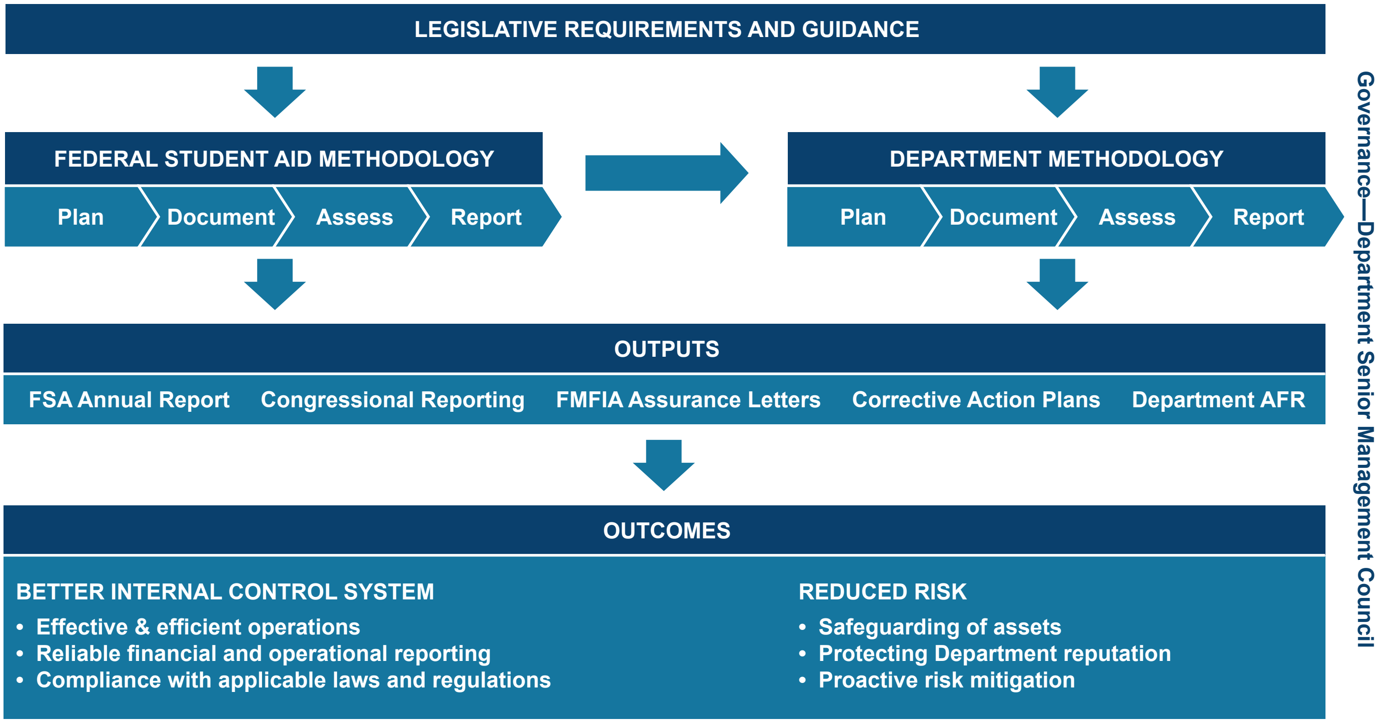
- *Operations*—Effectiveness and efficiency of operations.
- *Reporting*—Reliability of reporting for internal and external use.
- *Compliance*—Compliance with applicable laws and regulations.

This section describes the Department's internal control framework, offers an analysis of the effectiveness of its internal controls, and explains assurances provided by the Department's leadership that internal controls were in place and working as intended during FY 2020 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 GUIDANCE
FEDERAL STUDENT AID METHODOLOGY
Plan
Document
Assess
Report
DEPARTMENT METHODOLOGY
Plan
Document
Assess
Report
OUTPUTS
FSA Annual Report
Congressional Reporting
FMFIA Assurance Letters
Corrective Action Plans
Department AFR
OUTCOMES
BETTER INTERNAL CONTROL SYSTEM
• Effective & efficient 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

The Department continues to 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 (SMC). 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 that 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 as well as annual internal control training for all employees, to provide reasonable, but not absolute, assurance that its internal controls are well designed, 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 (GAO) 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 2020, 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. The Department acknowledges that it has areas of control that need further strengthening, such as those identified elsewhere in this report, as well as the major challenges identified by the Department's OIG in its FY 2021 Management Challenges report. As an example, data quality and reporting are a challenge identified by OIG. The Department, its grantees, and its subrecipients must have effective controls to ensure that reported data are accurate and complete. The Department relies on program data to evaluate program performance and inform management decisions. The establishment of a Data Quality Plan integrated into testing of controls is helping to address this challenge identified by the OIG.

In accordance with OMB Circular A-123, the Department also conducted a separate 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. Key activities include:

- Maintaining process documentation for the Department's significant business processes and subprocesses.
- Maintaining an extensive library of key financial, operations, and Information Technology (IT) controls.
- Providing technical assistance to principal offices to help them understand and monitor key controls.
- Refining the Data Quality Plan to improve reporting controls and data quality.
- Implementing a risk-based control testing strategy.
- Developing corrective action plans when internal control deficiencies are found and tracking progress against those plans.

In FY 2020, the Department tested 86 key financial controls for both grants and non-grants areas. The internal controls assessment detected some control deficiencies, but none that would rise to the level of material weakness. Corrective actions have been initiated for the deficiencies identified. In addition, numerous recommendations have been provided to process owners to strengthen internal controls in their processes, such as verifying immaterial differences, obtaining electronic signatures, and updating policies and procedures.

Further, operational internal controls have been formally aligned with the agency's overall ERM strategy and assessed accordingly. No control deficiencies have been reported for FY 2020 related to this assessment.

ANALYSIS OF FINANCIAL MANAGEMENT SYSTEMS

The *Federal Financial Management Improvement Act of 1996* (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 enhance financial reporting and compliance activities. The Department's core financial applications are together under common management control as part of the Education Central Automated Processing System (EDCAPS). EDCAPS is a suite of financial applications (subsystems), including commercial off-the-shelf, 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.
- Administrative processes (e.g., purchasing, travel, and miscellaneous payments).

EDCAPS is composed of four main integrated components:

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

Across all its components, EDCAPS is serving approximately 2,800 Departmental internal users in Washington, D.C. and 10 regional offices throughout the United States and territories. EDCAPS is serving approximately 40,500 external users, mostly users of the G5. In FY 2020, 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 2020:

- 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 (FFATA) and Digital Accountability and Transparency Act of 2014 (DATA Act)*.
- Transmitting the entire Department's payments through the Department of Treasury Secure Payment System.

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 Plan 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 (IPP).
- FSA-Financial Management System financial data.

- Lockbox.
- Department of the Treasury systems.
- 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 the Chief Counsel of the Department of the Treasury's Bureau of the Fiscal Service to interpret the impact of this revised *DATA Act*'s delinquent debt referral requirement on Title IV debt. In July 2015, the Fiscal Service's Chief Counsel determined 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 (TOP) referral requirement for Title IV debt owned by FSA at the time of delinquency is 271 days delinquent, and the requirement 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, 2020, the Department and FSA were not in compliance with the DCIA TOP 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 2020, FSA continued to implement changes to its default loan servicing systems, procedures, and internal business process for referring eligible debts to the Treasury Offset Program sooner. FSA will build DCIA requirements into the NextGen FSA servicing platform. This area of noncompliance is noted in the independent auditors' 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 2020 to improve cybersecurity capabilities and functions, some of which included:

- Office of the Chief Information Officer (OCIO) established the Department's cybersecurity risk tolerance and appetite which integrates with the Department's overall Enterprise Risk Management (ERM) program. Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) have been established to support tracking and reporting progress made towards the Department's OCIO ERM target profile.
- OCIO publishes monthly Department Cyber Security Framework (CSF) Risk Scorecards as part of the Department's Information Security Continuous Monitoring efforts to identify cybersecurity risks, issues, and opportunities for improvements in our cybersecurity protections. The Department CSF Risk Scorecard provides a detailed analysis tool for Authorizing Officials, Information System Owners, and Information System Security Officers to prioritize and mitigate risks to the Department's information systems.

- In FY 2020, the CSF Risk Scorecard was enhanced to include risk scoring and reporting for privacy controls as well as additional reporting views for the recently released security authorization documentation and incident response plan testing status scoring risk factors. These enhancements further enable the Department's stakeholders to effectively manage system level security and privacy risks while ensuring authorization documentation and processes are continuously monitored for effectiveness. CSF Risk Scorecard visualizations were also expanded upon to include specific views for FSA servicers and pertinent investment review board reporting to streamline communication of risk to appropriate stakeholders. These recent CSF Risk Scorecard enhancements have provided the Department's executives with new capabilities to identify trends, patterns, and opportunities for improvement across the organization. Additionally, the scorecard is now updated daily for a timely view of risk.

- OCIO disseminated monthly 'State of IT' principal office-level reports for continued outreach to executive stakeholders to take the appropriate actions as necessary based on cyber data, trends, metrics, and key insights specific to their organization offered through cybersecurity data visualizations.

- The average time to close a Plan of Action and Milestones (POA&M) was reduced from 167 days in 2019 to 47 days in 2020. The number of accepted POA&Ms also dropped from 53 to 29 during the same time period. At the closing of FY 2020, the Department achieved a 68 percent net reduction in past due POA&Ms since starting the reporting period on October 1, 2019.These positive metrics are direct indicators of the progress achieved in maturing risk management capabilities and reduction capabilities.

- OCIO authorized the FedRAMP compliant Splunk Cloud as the Department's cybersecurity data lake and began initial configuration for ingestion of Continuous Diagnostics and Mitigation and continuous monitoring data. Currently, ten data sources have been identified for initial operational capabilities. These enhancements allow for better cyber risk visibility and monitoring of Department information systems to enable prompt data driven decisions.

- To mitigate operational impacts of the COVID-19 pandemic, OCIO delivered Personal Identity Verification authentication (PIV-A) as alternative multi-factor authentication solution providing continuity of critical business functions. Additionally, OCIO identified, analyzed, and recommended a cloud-based solution to provide rapid expansion of the Department's VPN capacity supporting the workforce during COVID-19 telework phase. OCIO also performed outreach for increased vigilance during the COVID-19 telework phase. OCIO implemented proactive security monitoring of PIV-A VPN connections by utilizing new data-lake-based Security Information and Event Management (SIEM) software solution. Department employees have also been educated regarding increased phishing and other cybercriminal scams targeting a largely at-home workforce (stimulus checks, spoofing legitimate Government Health organizations, etc.).

- OCIO completed the enhancement of the Department's Network Access Control (NAC) capability for non-government furnished equipment (GFE) within the Department's new IT environment that is superior to capabilities that existed prior to the FY 2019 transition. This provides a foundation to further implement the Department's zero-trust architecture.

- To bolster the Department's email security, OCIO fully deployed and monitored the Office 365 (O365) email Data Loss Prevention (DLP) capability. This capability enhances the Department's overall DLP capabilities and works in concert with network and desktop DLP solutions. OCIO also deployed DLP desktop agents on nearly 100 percent of Department endpoint devices to further enhance the identification of personally identifiable information such as Social Security and credit card numbers. In FY 2020, the Department's DLP solution identified and blocked 9,809 emails which prevented potential sensitive personally identifiable information security incidents.

- Through enhanced reporting of email and web security posture, the Department was able to significantly increase U.S. Department of Homeland Security (DHS) Binding Operational Directive (BOD) 18-01 compliance from 54 percent to 100 percent for email security and 87 percent to 96 percent for Hypertext Transfer Protocol Secure (HTTPS) tracking. Additionally, there were no overdue critical or high vulnerabilities in FY 2020 for ED's public facing assets reported in accordance with DHS BOD 19-02 Cyber Hygiene.

- Cybersecurity and personnel security requirements were incorporated into the Department's acquisition regulations in December 2019. The Office of Acquisition Management issued Acquisition Alert 2020-01, "Education Acquisition Regulation Class Deviation: Cyber and Personnel Security Requirements for Contractors". This deviation ensures active contracts, solicitations, and future contracts communicate the Department's cybersecurity and personnel security requirements to contractors and prospective contractors.

- The Department deployed a "Report Phishing" button on March 25, 2020, to all Department email clients, allowing users to directly report suspicious emails to ED's Security Operations Center (EDSOC) with a single click of a button. Prior to deployment, the average reporting rate for simulated exercises in FY 2019 was 15.21 percent (the highest reporting rate was 27.82 percent in March 2019). A phishing exercise conducted in the third quarter of FY 2020 resulted in a 41 percent reporting rate, with 91 percent of those who reported using the new "Report Phishing" button. The highest reporting rate noted in FY 2020 was 52.5 percent in August 2020 in response to an exercise which appeared to contain an attachment. This was the highest reporting rate since the launch of the phishing program in FY 2014. The Department also improved its overall response time in reporting. During FY 2018 and FY 2019 exercises, the first report from an end user was within an average of two minutes of the exercise launch. In FY 2020, the first report was received within an average of one minute of the exercise launch. In the event the email was an actual attack, early notification would enable the Department to block the internet addresses or domains associated with the email and reduce the potential impact and risk.

- OCIO continued conducting quarterly Department-level system-tailored Incident Response and Contingency Plan testing tabletop exercises virtually, which focused on system contingency planning in the event of a cyber incident and how the Department would respond to such an incident. As of July 2020, 100 percent of the Department's FISMA reportable systems had a valid contingency plan test. Feedback reports were provided to system stakeholders on weaknesses and opportunities for improvement to their contingency plans:
  - Quarterly Risk Management Assessment score.
  - Department Cyber Risk score.
  - Previous year IG FISMA maturity score.
  - DHS Cyber Hygiene Scorecard.

- OCIO continued supporting the Scholarship for Service (SFS) program which is managed by the National Science Foundation in collaboration with the U.S. Office of Personnel Management (OPM) and DHS. This initiative reflects the critical need for IT professionals, industrial control system security professionals, and security managers in federal, state, local, and tribal governments. Upon graduation, scholarship recipients are required to work for a federal, state, local, or tribal government organization in a position related to cybersecurity. The Department spoke to students from SFS about the Department's internship and upcoming employment opportunities. Over 100 students stopped by to learn about the Department's cybersecurity initiatives and how their interests, knowledge, skills, and abilities aligned with future employment opportunities. OCIO continued to support the SFS program during COVID-19 by virtually onboarding a student internship team of eight students who performed a gap analysis, provided recommendations, and aided with next steps for adopting a Zero Trust Architecture environment at the Department.

- OCIO removed and blocked the Zoom video teleconferencing software across the enterprise after increased reports of security vulnerabilities. After thorough review of the risks associated with Zoom to Department users, updated guidance and notifications were communicated, allowing the use of Zoom for external hosted meetings with the understanding that there was no expectation of privacy, and meeting contents could be made public.

- OCIO nominated Subject Matter Experts (SMEs) to support the DHS Supply Chain Risk Management initiative, C-SCRM Cybersecurity Standards Innovation Group (CyberSIG). The SMEs contribute as key members of the CyberSIG under the sponsorship of the General Services Administration and OMB. The CyberSIG provides input into capabilities and requirements that will be used for C-SCRM government wide shared services.

- OCIO established initial operating capabilities in support of standing-up the Department's Information and Communications Technology SCRM program. An inter-agency agreement with the Department of Energy was established to use their operationalized enterprise SCRM program to help identify and reduce potential risks associated with third party vendor relationships. Through this shared service, the Department will receive vendor-specific risk assessment services for our information systems and our vendors.
- OCIO completed an engagement with the National Institute of Standards and Technology's (NIST) Security and Privacy Implementation Collaboration Tiger Team to integrate cybersecurity and privacy more effectively across government and to promote collaborative working relationships between cybersecurity and privacy, regardless of organizational structure/reporting. As a result of this engagement, NIST determined they will not include the collaboration index in revision 5 but will instead develop a template of the index as a supplemental resource for individualized agency use.