Analysis of Systems, Controls, and Legal Compliance

Management Assurances

Management Control Program

The Department's system of internal control is comprehensive and requires all Department managers to establish cost-effective systems of management controls to ensure U.S. Government activities are managed effectively, efficiently, economically, and with integrity. All levels of management are responsible for ensuring adequate controls over all Department operations. As such, the Department's management is responsible for managing risks and maintaining effective internal control.

The *Federal Managers' Financial Integrity Act* (FMFIA) requires the head of each agency to conduct an annual evaluation in accordance with prescribed guidelines and provide a Statement of Assurance (SOA) to the President and Congress. The Secretary of the Department of Education's Fiscal Year 2023 SOA provided below is the final report produced by the Department's annual assurance process.

SECRETARY'S STATEMENT OF ASSURANCE
FISCAL YEAR 2023
November 16, 2023

The Department of Education's (the Department's) 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 (DQP) in accordance with Appendix A of OMB Circular A-123.

The Department's management is responsible for managing risks and maintaining effective internal control to meet the objectives of Sections 2 and 4 of the FMFIA. The Department conducted its assessment of risk and internal control in accordance with OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control. Based on the results of the assessment, the Agency can provide modified assurance that internal control over operations, reporting, and compliance were operating effectively as of September 30, 2023, due to the following material weakness:

The material weakness is related to the subsidy estimate for the Department's Direct Loan (DL) and Federal Family Education Loan (FFEL) student loan portfolios. The Department is required to perform interest rate and technical re-estimates of the subsidy costs (commonly referred to as subsidy re-estimates) of its direct loan and loan guaranty programs as of September 30th every year. These subsidy re-estimates

are calculated using an internally developed cash flow model, the Student Loan Model (SLM). In FY 2023, the external financial statement auditor and FSA separately identified errors in the data in the system that was used in key assumptions for the SLM. FSA has corrected some of the identified errors and is continuing to research other known issues to identify and implement corrective actions.

Miguel A. Cardona, Ed.D.

Introduction

The FMFIA requires the Government Accountability Office (GAO) to prescribe standards of internal control in the Federal Government, which is titled *GAO's Standards for Internal Control in the Federal Government* commonly known as the Green Book. These standards provide the internal control framework and criteria Federal managers must use in designing, implementing, and operating an effective system of internal control. The Green Book defines internal control as a process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity are achieved. These objectives and related risks can be broadly classified into one or more of the following categories:

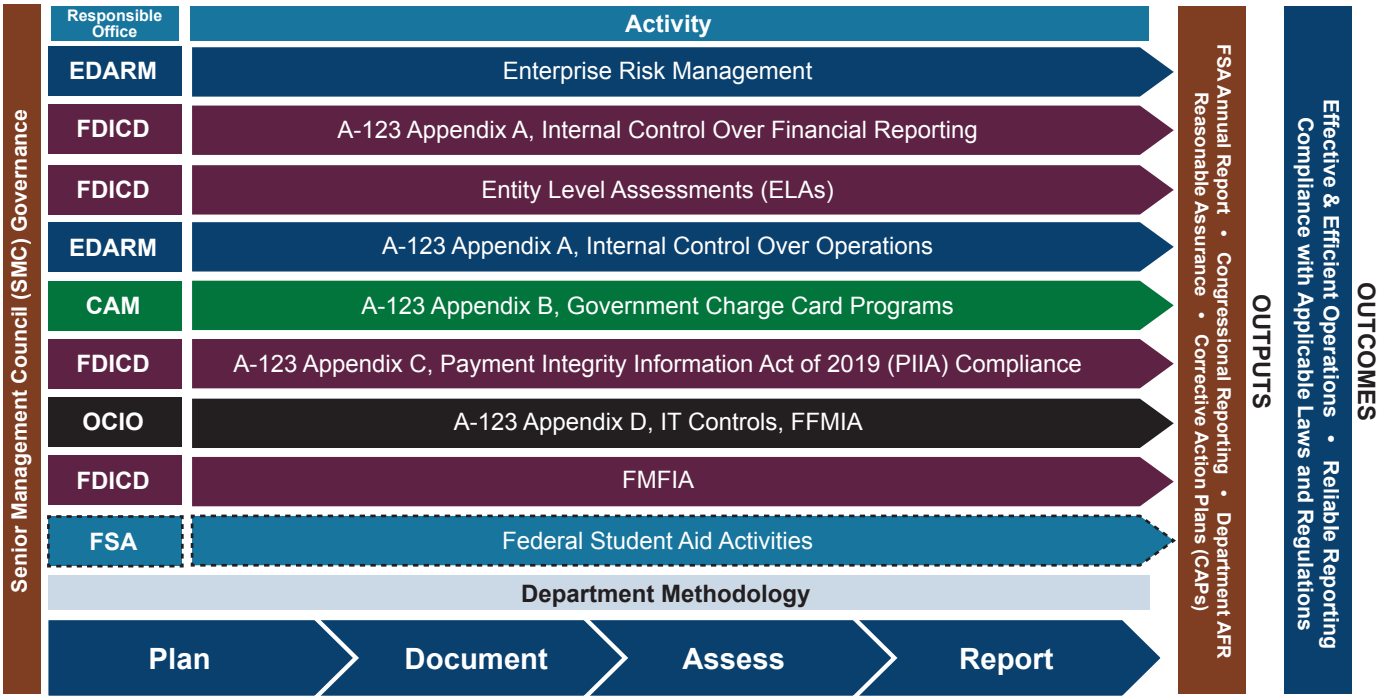
- *Operations*—Effectiveness and efficiency of operations.
- *Reporting*—Reliability of reporting for internal and external use.
- *Compliance*—Compliance with applicable laws and regulations.

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 and mission-support operations. This is achieved through implementation of ERM practices and by establishing, maintaining, and assessing internal control effectiveness. Furthermore, the guidance requires federal agencies to provide reasonable assurance that it has met the three objectives of internal control. This section describes the Department's internal control framework and explains assurances provided by the Department's leadership.

Internal Control Framework

The Department's internal control framework helps 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's comprehensive internal control framework and assurance process is depicted in the following diagram in Figure 13.

Figure 13. Department of Education Internal Control Framework



EDARM Division of Enterprise Data Analytics and Risk Management
FDICD Financial Data Integrity and Controls Division
CAM Contracts & Acquisitions Management
FMFIA Federal Managers' Financial Integrity Act of 1982
OCIO Office of the Chief Information Officer
FSA Federal Student Aid

The Department worked to evolve its existing internal control framework to be more value-added and provide for stronger risk management for the purpose of improving mission delivery. The Department's Senior Management Council (SMC) oversees the Department's management control program. Individual SOAs from Assistant Secretaries in Principal Office Components (POCs) serve as the primary basis for the Department's FMFIA SOA issued by the Secretary. The SOAs are based on information gathered from various sources including managers' personal knowledge of day-to-day operations and existing controls, management program reviews, and other management-initiated evaluations. In addition, the Office of Inspector General and the GAO conduct reviews, audits, inspections, and investigations that are considered by management.

The Department's Office of Finance and Operations (OFO) employs an integrated process to perform the work necessary to meet the requirements of OMB Circular A-123's Appendix A and Appendix C (regarding Payment Integrity), the FMFIA, and GAO's Green Book. Green Book requirements directly relate to testing entity-level controls, which is a primary step in operating an effective system of internal control. Entity-level controls reside in the control environment, risk assessment, control activities, information and communication, and monitoring components of internal control in the Green Book, which are further analyzed by 17 underlying principles of internal control. For the Department, all five internal control components and 17 principles were assessed in support of the Department's FY 2023 SOA.

The Department employs a risk-based approach in evaluating internal controls over reporting on a multi-year rotating basis, which has proven to be efficient. Due to the broad knowledge of management involved with the Appendix A assessment, along with the extensive work performed by the divisions who assess key controls, the Department was able to evaluate issues on a detailed level. The Department's management controls program is designed to ensure full compliance with the goals, objectives, and requirements of the FMFIA and various Federal laws and regulations. Numerous Department organizational entities provided oversight during FY 2023 for the internal controls over reporting program in place to meet the requirements of OMB Circular A-123, Appendix A. These entities include the Division of Enterprise Data Analytics and Risk Management (EDARM), Financial Data Integrity and Controls Division (FDICD), Contracts and Acquisitions Management (CAM), Office of the Chief Information Officer (OCIO), and Federal Student Aid (FSA). To that end, the Department has dedicated considerable resources to administer a successful management control program. As noted in the Secretary's Statement of Assurance, the Department identified one material weakness in control operation and design.

The Department also places emphasis on the importance of continuous monitoring. It is the Department's policy that any organization with a material weakness or significant deficiency must prepare and implement a corrective action plan to correct the weakness. The plan, combined with the individual SOAs and Appendix A assessments, provide the framework for monitoring and improving the Department's management controls on a continuous basis. Management will continue to direct and focus efforts to resolve any deficiencies in internal control identified by management and auditors.

The Department continues to focus on streamlining and coordinating internal control activities to ensure efficiency of operations, recognize the connection points across areas, and enable transparency of information across the Department. This framework enables increased compliance, process efficiency, oversight, and more informed monitoring of internal controls and risk management by all offices and governance bodies, including the Department's Senior Management Council. The framework also allows for the Department to obtain outcomes from an improved control system and 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; internal controls are in place and working as intended; and operations are efficient and effective.

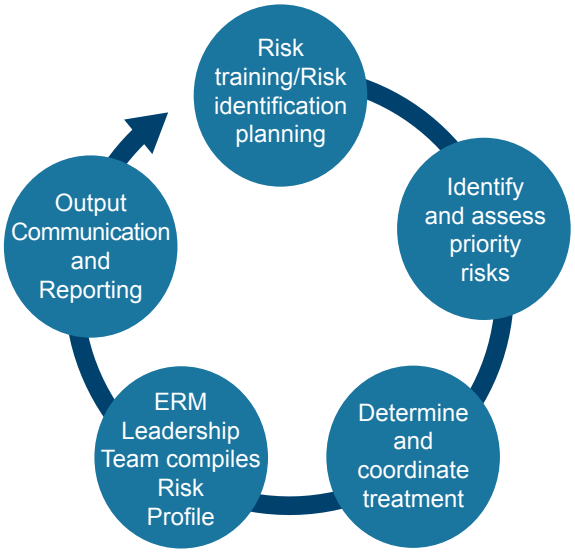
Additionally, during FY 2023, the Department continued taking important steps to advance its Enterprise Risk Management (ERM) program.

Enterprise Risk Management Framework

The Department's Enterprise Risk Management (ERM) program supports agency-wide efforts to maximize the Department's value to students and taxpayers through achievement of strategic goals and objectives. The Department's ERM program strategically focuses on the complete spectrum of the organization's significant risks and the combined impact of those risks as an interrelated portfolio rather than simply addressing risks within silos. This coordinated approach leverages data and analytical solutions to identify, measure, and assess challenges related to mission delivery and resource management. Through ERM, the Department has established a systematic and deliberate view of risk into key management practices, ultimately yielding more effective performance and operational outcomes.

The Division of Enterprise Data Analytics and Risk Management (EDARM), within the Office of Finance and Operations (OFO), leads the agency's overall ERM strategy and formally aligns ERM and internal controls processes. EDARM leverages partnerships with agency leaders (e.g., the Senior Management Council, the Senior Executive Cadre, political leadership) to identify, measure, and assess challenges related to mission delivery, policy development, and operations to develop coordinated, actionable response plans.

The ERM Annual Assessment process includes the following key steps:



EDARM collaborated with every Principal Office Component (POC) to identify and evaluate risk priority within each POC and at the Department-wide level. The FY 2023 Department of Education ERM profile was published with the aggregated result and analysis from the annual assessment process. This profile highlights the top 15 risks for the Department around the following 6 main functional processes:

- *Financial Management:* Student Loan Cost Estimation, Budget Formulation.
- *Human Capital Management:* Recruitment & Hiring, Workforce & Succession Planning, Employee Training & Development, Employee Engagement & Retention.
- *Information Technology Management:* IT Process Governance, Cybersecurity, and Infrastructure.
- *Business Process Management:* Acquisition/Budget Strategy.
- *Data Management*: Information Security and Data Protection, Data Quality.
- *Oversight and Compliance:* Grants and Contracts Management.

In FY 2023, after launching the ERM digital tool for collecting, analyzing, and reporting risk data, EDARM continued to enhance the tool based on user feedback and is building additional capabilities and visual analysis for all stakeholders to further monitor and evaluate trends and results.

EDARM continues to make progress in developing and implementing new trainings, tools, and helpful content to better educate and promote healthy risk culture, a culture of continuous improvement within the Department—where data and awareness of enterprise risk are used to objectively inform strategic and operational decisions and optimize agency performance.

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 provided for all employees—to demonstrate 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 Green Book and OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*.

In FY 2023, the Department and Federal Student Aid (FSA) did identify one material weakness related to the reliability of reporting. The Department acknowledges that it has areas of control that need further strengthening, as well as major challenges identified by the Department's Office of Inspector General (OIG) in its FY 2024 Management Challenges report. As an example, data quality and reporting are a challenge identified by the 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 (DQP) integrated into testing of controls is helping to address this challenge identified by the OIG.

The Department maintains processes and procedures to identify, document, and assess internal control over reporting and operations. Key activities include:

- Maintaining process documentation for the Department's significant business processes and subprocesses.
- Maintaining an extensive library of key financial, operational, and information technology (IT) controls.
- Providing technical assistance to principal offices to help them understand and monitor key controls.
- Refining the DQP 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.
- Recommending and assisting with implementation of robust tools to design more efficient and effective operating procedures.

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,

operations, and compliance with key financial management laws and regulations, as described below.

Internal Control Over Reporting

Annually, the Department evaluates its POCs' internal control system using the 17 GAO Green Book principles to ensure entity level control objectives are met. These evaluations assist POCs in producing a letter of assurance each year by September 30, documenting their internal control system, identifying any control deficiencies, and noting any major improvements or challenges.

In FY 2023, the external financial statement auditor and FSA separately identified errors in the data in the system that was used in key assumptions for the SLM. FSA has corrected some of the identified errors and is continuing to research other known errors to identify and implement corrective actions.

In FY 2023, the Department tested a proportionate number of key financial controls in significant business processes based on qualitative process risk assessments and rotational test plans. The internal controls assessment did not find any material weaknesses. However, recommendations have been provided to process owners to strengthen internal controls, such as verifying immaterial differences, obtaining electronic signatures, and updating policies and procedures.

In addition, the Department's shared service provider, the U.S. Department of the Interior (DOI)/ Interior Business Center (IBC), uses the Federal Personnel and Payroll System (FPPS) to process its payroll. DOI's auditor tested FFPS and the results of their FY 2023 review indicated that the controls tested were operating effectively, providing reasonable assurance that the control objectives specified were achieved during that period.

Internal Control Over Operations

In FY 2023, the Department reviewed a number of operational processes based on qualitative risk assessments (in alignment with the Department's ERM profile) and detected some control deficiencies but none that would rise to the level of material weakness. As a result, tools have been developed in the areas of stakeholder outreach, acquisition planning and the procurement process to better utilize resources, improve the flow, timeliness, and quality of information, and allow for more effective decision-making. A significant achievement has been the creation of the acquisition portal and dashboard, which enhances and streamlines the acquisition management process by providing a solitary access point for gathering, editing, and reviewing submissions and enabling accountability and transparency throughout the Department. The dashboard provides the Department with the ability to present decision-makers with clearly understood data to spot important acquisition trends and resources across the agency.

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 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 FFMIA, 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 integrated 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:

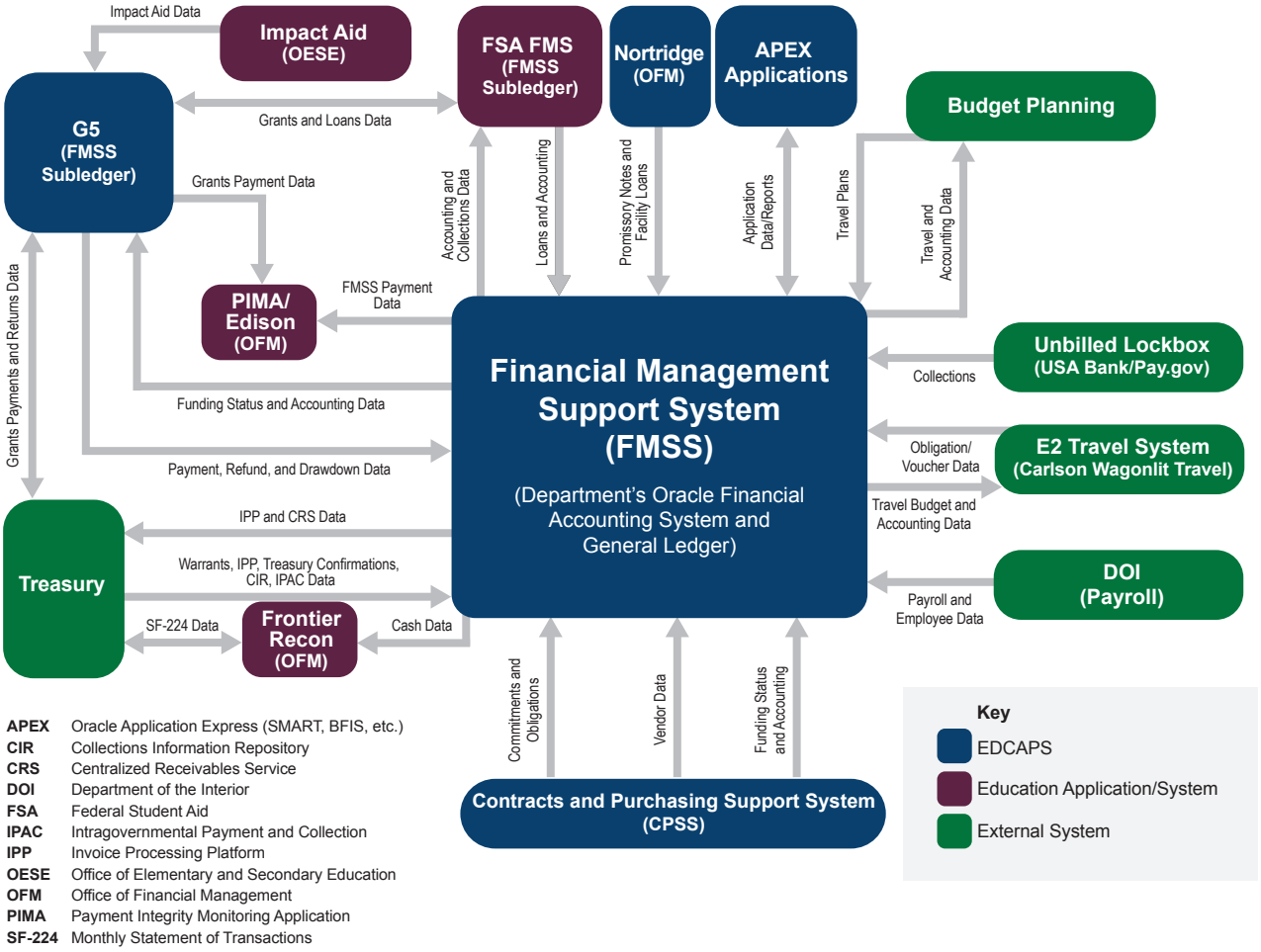
- General ledger—Preparation of financial statements and reconciliation of general ledger balances with subsystems maintained in program areas and Treasury.
- Funds management—Budget formulation, budget execution, and funds control.
- Grants pre- and post-award processing, including grant payment processing.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

EDCAPS is composed of five main integrated components:

- Financial Management Support System (FMSS)—FMSS is the Department's core financial system. It provides financial management functions such as the general ledger, financial statement preparation, funds control and budget execution, purchase receiving, accounts receivable, and accounts payable.
- The FMSS Oracle E-Business Suite application resides behind the Department firewall and is not an external-facing application.
- Contracts and Purchasing Support System (CPSS)—CPSS provides the Department with a central repository to enter, retrieve, manage, and view acquisition/contract-related data. The centralized data provides enhanced information dissemination, with the ability to respond to both internal and external information requests.
- Grants Management System (G5)—G5 provides the Department with a platform to manage all grant activities, from initial recipient contact to grant processing to payments and grant closeout. This single-system approach provides improved grant information management, recipient response time, and accuracy of financial management information.
- E2 Travel System—E2 provides the Department, under a GSA contract with third party, with a platform to manage travel functions. EDCAPS interfaces with E2 in accordance with an established Memorandum of Understanding and Information Security Agreement between the Department and the vendor.

The following diagram provides the data flow in and out of EDCAPS, including data flow with other Department applications/systems and external applications/systems.

EDCAPS (FMSS) Functional Flow Diagram



APEX	Oracle Application Express (SMART, BFIS, etc.)
CIR	Collections Information Repository
CRS	Centralized Receivables Service
DOI	Department of the Interior
FSA	Federal Student Aid
IPAC	Intragovernmental Payment and Collection
IPP	Invoice Processing Platform
OESE	Office of Elementary and Secondary Education
OFM	Office of Financial Management
PIMA	Payment Integrity Monitoring Application
SF-224	Monthly Statement of Transactions

Across all its components, EDCAPS is serving numerous Departmental internal users in Washington, D.C. and 10 regional offices throughout the United States and territories, as follows:

- G5 – 825
- CPSS - 710
- FMSS - 400
- E2 – 3,720

EDCAPS is serving approximately 45,790 external users, mostly users of Grants Management System (G5). In FY 2023, the Department conducted an annual risk assessment of EDCAPS and tested 86 IT security controls out of a baseline of 630 IT security controls, as follows:

- EDCAPS—15
- FMSS—3
- CPSS—27
- G5—33
- E2—8

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 2023:

- 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* and *Digital Accountability and Transparency Act of 2014.*
- 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 external systems:

- Department Systems:
  - Oracle Enterprise Performance Management Cloud Planning (formerly Hyperion).
  - Fiserv Frontier.
  - G5.
  - CPSS.
- External Systems:
  - Treasury systems (Invoice Processing Platform [IPP] invoices/receipts/obligation data, IPP invoice status, payment files, debt referrals, Centralized Receivables Service invoices, warrants, Treasury confirmations, Collections Information Repository collections and administrative return, collections/payments).
  - E2 Travel System.

The Department's financial management systems are designed to support effective internal control and produce accurate, reliable, and timely financial data and information, except for the material weakness reported in the Secretary's Statement of Assurance. The financial

statement auditors, in their independent assessment, concluded that the Department did not substantially comply with FFMIA requirements, and the Department concurred. 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. However, the Department reports some areas of non-compliance:

The Federal Managers' Financial Integrity Act (FMFIA)

Federal Managers Financial Integrity Act of 1982 (FMFIA), Pub. L. 97-255 – (H.R. 1526) was enacted into law on September 8, 1982.

The FMFIA establishes overall requirements with regard to internal control and requires the agency head to certify annually to the President and Congress whether there is reasonable assurance that the Department's internal controls are achieving their intended objectives. This is also noted in the Office of Management and Budget Circular A-123 (OMB A-123), *Management's Responsibility for Enterprise Risk Management and Internal Control*, which implements the FMFIA.

The Department's management performed an internal control assessment as required under FMFIA; however, management's assessment did not comply with limited requirements within the FMFIA and the related OMB A-123 requirements. Specifically, the Department did not identify and document specific and limited financial statement risks and the associated controls that were responsive to those specific risks. Additionally, the Department's management internal controls did not properly identify specific risks impacting the data used to calculate the subsidy re-estimates used in the consolidated financial statement. This resulted in the lack of timely identification of errors in data that impacted subsidy re-estimates in the consolidated financial statements.

Federal Financial Management Improvement Act of 1996 (FFMIA)

Federal Financial Management Improvement Act of 1996 (FMFIA), Pub. L. 104-208, Title VIII (31 U.S.C. 3512 note) was enacted into law on September 30, 1996.

The FFMIA requires the Department to establish and maintain financial management systems that comply substantially with Federal financial management systems requirements, applicable Federal accounting standards, and the United States Government Standard General Ledger at the transaction level. Appendix D to the Office of Management and Budget (OMB) Circular A-123 provides the FFMIA Compliance Determination Framework that is used in determining whether the Department's financial management systems comply substantially with FFMIA requirements. Per section 806 of the FFMIA, "financial management systems" includes the financial systems and the financial portions of mixed systems necessary to support financial management, including automated and manual processes, procedures, controls, data, hardware, software, and support personnel dedicated to the operation and maintenance of system functions.

The Department did not meet limited FFMIA requirements due to an inadequate risk assessment over specific key processes and data used in the consolidated financial statement. As a result, the Department did not comply with FFMIA, increasing the risk that transactions are incorrectly recorded to the general ledger, impacting the completeness, existence, and accuracy of the balances in the consolidated financial statement.

Payment Integrity Information Act of 2019 (PIIA)

The ***Payment Integrity Information Act of 2019 (PIIA), Pub. L. 116-117, 134 Stat. 113***, was enacted into law on March 2, 2020.

The primary purpose of the PIIA is to reorganize and revise several existing improper payments statutes,[3] which establish requirements for federal agencies to cut down on improper payments made by the federal government. PIIA requires federal agencies to report improper payments annually for programs that are deemed susceptible to significant improper payments. PIIA also requires each agency's OIG to review the agency's improper payment reporting in its Agency Financial Report (AFR) and accompanying materials, and to determine whether the agency has met six compliance requirements.

In its annual improper payment compliance audit for FY 2022, the OIG concluded that the Department did not comply with the PIIA for the FY 2022 reporting period because it did not meet one of the six compliance requirements. Specifically, the Department reported improper payment and unknown payment estimate rates that exceeded 10 percent.

For the Title I program, the Department reported an improper payment and unknown payment estimate that exceeded 10 percent for the second consecutive year. To comply with 31 U.S.C. section 3351(2)(F), an agency must report an improper payment rate of less than 10 percent for each program and activity for which an estimate was published. In addition, the Department's OIG determined that the improper payment and unknown payment estimates for each of the five programs (Title I, Special Education, Education Stabilization Fund, Pell Grant, and Direct Loan) were not reliable. Specifically, for the Title I and Special Education programs, the improper payment and unknown payment estimates were based on inaccurate sampling populations. Further, for the Title I, Special Education, and Education Stabilization Fund programs, the Department's testing results were inaccurate.

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

Additionally, auditors determined that the Department's overall IT security program and practices are effective, as eight out of the nine FISMA domains met the requirements needed to operate at a Level 4 maturity rating, indicating the systems security is Managed and Measurable.

Federal Information Security Modernization Act of 2014 (FISMA)

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 relevant information technology systems. The Act supports the operations and assets of the agency and helps to ensure the confidentiality, integrity, and availability of all system-related information.

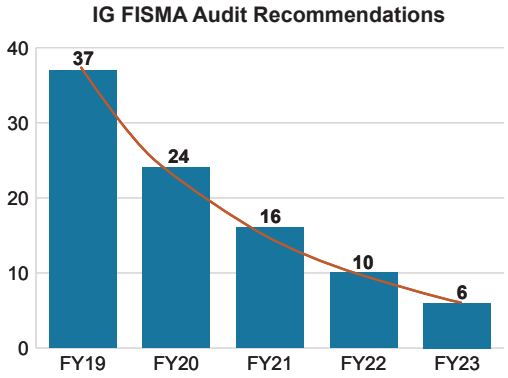
The Department's and FSA's information security programs completed numerous significant activities in FY 2023 to improve cybersecurity capabilities and functions, some of which include:

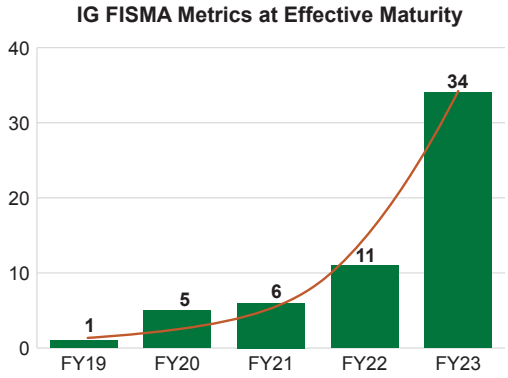
- In FY 2022, the Department received an overall FISMA assessment of "Effective," or a Level 4 Cybersecurity Maturity Level. This score was the highest achieved by

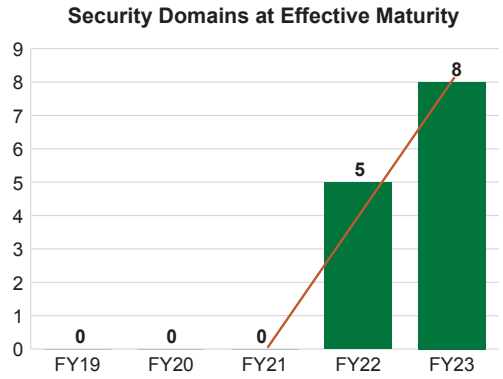
3 *Improper Payments Information Act of 2002 (IPIA), Pub. L. 107-300, 116 Stat. 2350*, as amended by the *Improper Payments Elimination and Recovery Act of 2010 (IPERA), Pub. L. 111-204, 124 Stat. 2224,* and *the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA), Pub. L. 112-248, 126 Stat. 2390.*

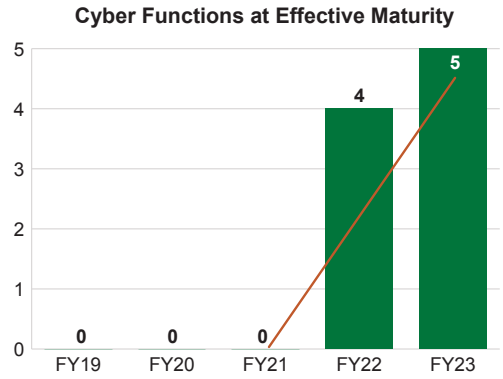
the Department since the scoring metrics were established in 2014. In FY 2023, the Department was again assessed to be overall "Effective." However, in FY 2023, all five cybersecurity functions were assessed to be operating at Level 4. This is the first time the Department has achieved such a result which reflects significant strides in advancing the Department's cybersecurity maturity and effectiveness across all functions and 8 of 9 security domains which make up those functions as supported by information in the graphics below.

Security Function	Metric Domain	Maturity Level	Change from 2022	Met Federal Goal
Identify	Risk Management	Managed and Measurable	▲	✓
Identify	Supply Chain Risk Management	Managed and Measurable	▲	✓
Protect	Configuration Management	Managed and Measurable	=	✓
Protect	Identity and Access Management	Consistently Implemented	=	
Protect	Data Protection and Privacy	Managed and Measurable	▲	✓
Protect	Security Training	Managed and Measurable	=	✓
Detect	Information Security Continuous Monitoring	Managed and Measurable	=	✓
Respond	Incident Response	Managed and Measurable	=	✓
Recover	Contingency Planning	Managed and Measurable	=	✓









- In FY 2023, the Department continued advancing its cybersecurity capabilities, policies, and procedures as well as implementing priority capabilities to reduce risk in support of requirements levied from Office of Management and Budget (OMB) and Department of Homeland Security (DHS), including those documented within Executive Order on Improving the Nation's Cybersecurity (EO 14028). The Department was the first cabinet-level Department to receive funding from the TMF and successfully adopted a SASE solution in support of advancing its ZTA capabilities in support of federal requirements as outlined in OMB Memorandum M-22-09. SASE has modernized the Department's cybersecurity posture through migrating away from legacy Virtual Private Networks (VPN). The new solution leverages cloud native capabilities to enhance the teleworking employees' experiences, including providing 10x faster connection speed than the legacy VPN access, reducing the number of logins required for applications, and increasing performance for tools such as Microsoft Teams, Outlook, Zoom, and other applications and data while modernizing the Department's Cybersecurity posture.

- The Department issued a contract with a professional service provider to modernize and enhance its Enterprise ICAM (Identity, Credential, and Access Management) solution beginning in September 2022 and aligns with the OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles requirements to meet specific cybersecurity standards and objectives by the end of FY 2024. The ICAM program continues to provide improved security features and functionality which enhance the security posture of the Department. The Enterprise ICAM service has been working to integrate all Department information systems with modern, phishing resistant authentication services, and has instituted a single sign-on (SSO) capability through a centralized user portal for Department employees and contractors to access their Microsoft Office 365 applications.

  - Enterprise ICAM provides the following new capabilities to the Department: self-service password reset functionality and security information registration; certificate-based authentication to support native personal identity verification (PIV) in cloud service provider SSO; and identity lifecycle management capabilities to enable automated user account provisioning and deprovisioning. Enterprise ICAM has also integrated with the ED Cyber Data Lake (EDCDL) to develop a centralized identity dashboard to improve transparency into identity related metrics that align with OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, and OMB Memorandum M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents, for user and privileged user logging requirements.

  - The Department's ICAM program was successful in integrating with Login.gov for public users and was integral to instituting multifactor authentication (MFA) deployment across the Department through integrating PIV validation of Department organizational users. Through the implementation of ICAM, Department online resources are more secure for users to access through implementation of phishing resistant authentication and improved visibility. Implementation also strengthens the Department's access management capabilities by reducing the risk of successful phishing cyber-attacks across the Department's enterprise and ensuring the right people have the right level of access to Department resources. Users experience a superior interaction with the Department's services as they will log on substantially fewer times and will need to remember fewer passwords and pins.

- The Department's accomplishments in maturing its risk management capabilities, specifically the maturation of the Cybersecurity Framework (CSF) Risk Scorecard, has been recognized by other Federal Agencies, including OMB, as an optimized capability in managing and communicating cybersecurity risk. The Department of Commerce, Department of Justice, Department of Transportation, and Nuclear Regulatory Commission have all requested playbooks for the development and implementation of CSF-based risk scoring capabilities in their environments based upon our constructs. Released in November 2022, version 3.0 of the ED CSF Risk Scorecard now aligns National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 5 security and privacy controls to the NIST CSF objectives as well as the NIST Privacy Framework (PF) Ver. 1.0. The ED CSF Risk Scorecard provides continuous measurement and risk prioritization of key metrics for system stakeholders, POC leadership, and Department executive leadership on a daily, monthly, and quarterly basis.

- On April 14, 2022, the Department's CISO issued a memorandum for Recission of Department Standard PR.AC: Emergency PIV Alternative. On May 5, 2020, to address the closure and limited operating capacity of Federal Government badging offices due to the coronavirus 2019, OCIO issued Standard PR.AC: Emergency PIV Alternative Standard. This standard provided authorization to access Department systems for those who did not hold a valid PIV but have been cleared by the Department's Office of Personnel Security. OCIO has determined Standard PR.AC: Emergency PIV Alternative Standard is now unnecessary as Federal Government badging offices are now open and are at normal operating capacity. This memo serves to drive actions necessary to ensure the Department's workforce is using the strongest multifactor authentication possible in alignment with Executive Order 14028.

- The integration of supply chain risk management (SCRM) assessments with the Department's Enterprise Architecture Technology Insertion process, also known as the (EATI) process, successfully identified 15 CFR Part 7 concerns with Eclipse DB and 7-zip resulting in Deep Dive reviews and the creation of plan of action and milestones for mitigation. SCRM has also been integrated into the CSF Risk Scorecard to strengthen the ability to measure and monitor supply chain risk. This integration has allowed the Department to identify risks and empowered senior leadership the ability to accept, mitigate, or transfer supply chain risk appropriately within the Department.

- The Department continued to build on FY 2022 awards and received multiple recognitions and multiple awards in FY 2023 from the Federal Information Security Educators Association (FISSEA). FISSEA is an organization run by and for Federal government information security professionals to assist Federal agencies in strengthening their employee cybersecurity awareness and training programs. These awards include Awareness Training Category award for the Cybersecurity and Privacy Awareness Escape Room course; Innovative Solutions award for badges awarded for high levels of symposium participation and top reporters of phishing exercises; and Awareness Newsletter award for the Department's Bits and Bytes awareness newsletter. Following receipt of these awards, the Department of Energy, Postal Regulatory Commission, Social Security Administration, Department of Health and Human Services, Department of Labor, Department of Commerce, and Consumer Financial Protection Board reached out to the Department and requested meetings to learn more about the Department's program and obtain guidance and direction on how to build and maintain an effective training program.

- From an incident response perspective, there have been no major cybersecurity incidents across the Department in FY 2023. To bolster collaboration and interagency coordination, the Department has also allocated a dedicated resource to work with law enforcement and the National Cyber Investigative Joint Task Force. The Department also continued maturing its cyber threat intelligence and cyber hunt capabilities by establishing dedicated resourcing to interface with the intelligence community for Department of Education-specific threat indicators.

- The Department, in coordination with 18 Federal agencies through the Memorandum 21-31 (M-21-31) working group, is leading the government's efforts to determine impact, applicability, and legal ramifications for statistical data collection for event logging. Adhering to Executive Order (EO) 14028 (Section 8) to improve the Nation's Cybersecurity, the implementation M-21-31 will strengthen the Department's event logging capabilities to better identify, investigate and prevent cyber-attacks such as data breaches, identity theft, and other types of cybercrime. Without this capability, the Department will be unable to aid law enforcement and national security partners when a cyber-attack impacts the Department. This can lead to prolonged attacks degrading, disrupting, and limiting services. Furthermore, Department staff will be unable to answer questions to Congress and oversight bodies about what happened, when it started, and how staff resolved the issue in cybersecurity breaches and incidents.

- On February 27, 2023, OMB Memorandum M-23-13, "No TikTok on Government Devices" Implementation Guide, was issued. The Department issued the appropriate CISO memorandum to all Department employees and contractors to remove TikTok and any successor application or service developed or provided by ByteDance Limited or subsidiary from ED devices and providing instructions and deadlines for its removal. Further the Department was able to leverage its newly deployed ZTA tools, SASE, to begin blocking TikTok by its application identifier.

- In support of the Department's maturation plan for the Education's Security Operations Center (EDSOC), efforts are underway to build out a consolidated and centralized SCIF for use by the Department and FSA. This new SCIF will provide a secure room for classified briefings as well as serve as a disaster recover site to ensure continuity of business operations in the event of an emergency and deemed necessary.

  - In February 2023, the Department and FSA combined Security Information and Events Management licenses and migrated FSA's data to the EDCDL in August 2023. In doing so, the Department saved in FY 2023, this migration drastically increased the opportunity for information sharing between EDSOC and FSA Security Operations Center incident response analysts allowing the Department to adhere to EO 14028 and OMB M-21-31.

  - The Department also enhanced its data loss prevention (DLP) capability through an engagement with DHS CISA under the Secure Cloud Business Applications project which provided guidance and capabilities to secure cloud business application environments and protect federal information that is created, accessed, shared, and stored. The Department has also gone above and beyond by taking the next steps to include DLP looking for things like Federal Tax Information and Employer Identification Number.

- The Department's Information System Security Support Services (I4S) executed a Blanket Purchase Agreement (BPA), as well as I4S BPA Call Order1 to provide Support Services related to Program Management Support, Governance, Risk and Compliance Tool (CSAM) Support, and Contractor Information System Security Officer (ISSO) Support. The Department will now be able to execute call orders against this BPA to procure Information System Owner, ISSO, and Vulnerability Management and Security Engineering services.