Analysis of Systems, Controls, and Legal Compliance

MANAGEMENT ASSURANCES

The Secretary of the Department of Education's Fiscal Year 2022 Statement of Assurance provided below is the final report produced by the Department's annual assurance process.

STATEMENT OF ASSURANCE
FISCAL YEAR 2022
January 23, 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 Federal Managers' Financial Integrity Act. 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 reasonable assurance that internal control over operations, reporting, and compliance were operating effectively as of September 30, 2022.

Miguel A Cardona

Miguel A. Cardona, Ed.D.

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 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:

- *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, and explains assurances provided by the Department's leadership.

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.

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 2022 Department of Education ERM profile was published with the aggregated result and analysis from the annual assessment process. This profile highlights the top 11 risks for the Department around the following 5 main functional processes:

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

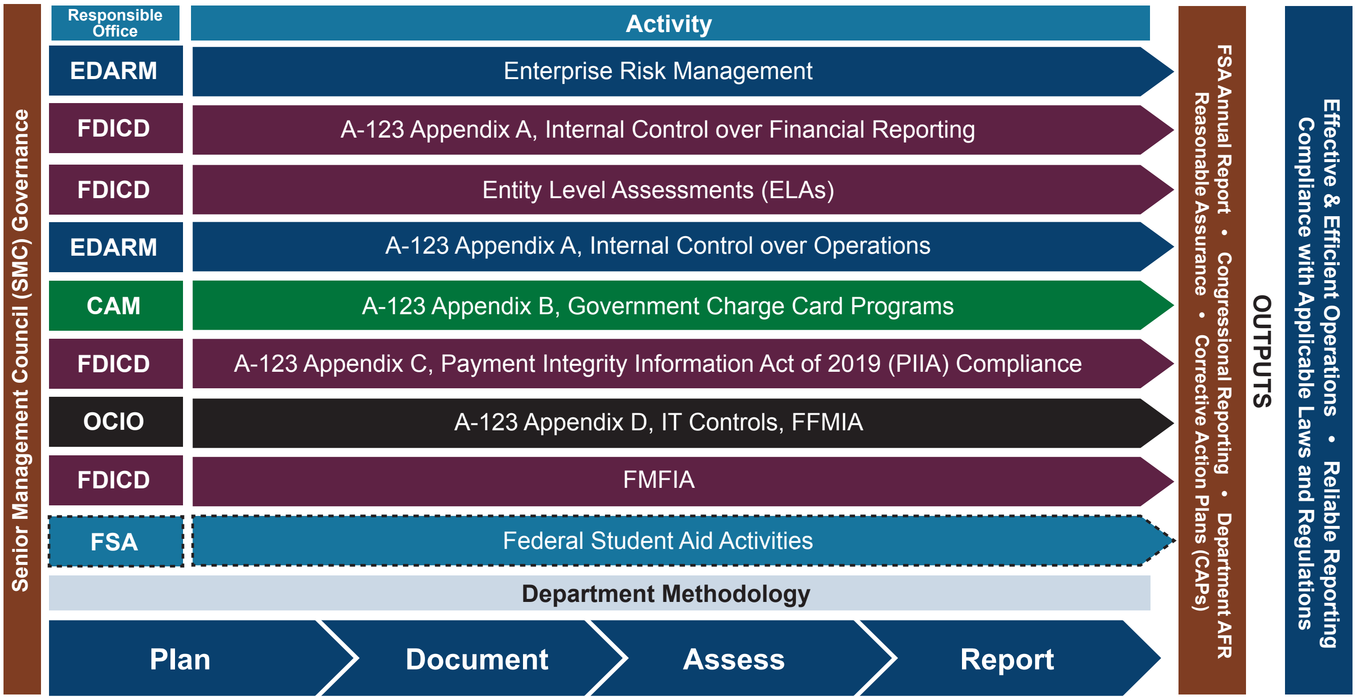
In FY 2022, EDARM also launched the ERM digital tool for collecting, analyzing, and reporting risk data to promote transparency and accountability across the Department.

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.

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 13. Department of Education Internal Control Framework



Senior Management Council (SMC) Governance

Responsible Office	Activity
EDARM	Enterprise Risk Management
FDICD	A-123 Appendix A, Internal Control over Financial Reporting
FDICD	Entity Level Assessments (ELAs)
EDARM	A-123 Appendix A, Internal Control over Operations
CAM	A-123 Appendix B, Government Charge Card Programs
FDICD	A-123 Appendix C, Payment Integrity Information Act of 2019 (PIIA) Compliance
OCIO	A-123 Appendix D, IT Controls, FFMIA
FDICD	FMFIA
FSA	Federal Student Aid Activities

Department Methodology

Plan → Document → Assess → Report

OUTPUTS

FSA Annual Report • Congressional Reporting • Department AFR
Reasonable Assurance • Corrective Action Plans (CAPs)

OUTCOMES

Effective & Efficient Operations • Reliable Reporting
Compliance with Applicable Laws and Regulations

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 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.

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 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 2022, the Department and Federal Student Aid (FSA) did not self-identify any material weaknesses related to the effectiveness and efficiency of its operations. However, an area of noncompliance with laws and regulations is noted in the Analysis of Legal Compliance section below. 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 the Inspector General (OIG) in its FY 2023 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

In FY 2022, the Department tested a proportionate number of key financial controls in significant business processes in non-grant areas based on qualitative risk assessments and rotational test plans. The internal controls assessment did not find any control deficiencies or material weakness. 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.

Internal Control Over Operations

In FY 2022, 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 workforce planning, 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 major accomplishment has been the development of a workforce dashboard that consolidates relevant and up-to-date human resources data from multiple systems in a single location and visually depicts complex relationships in an easily digestible manner, enhancing decision-makers' ability to identify critical human resource trends and challenges across the Department.

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:

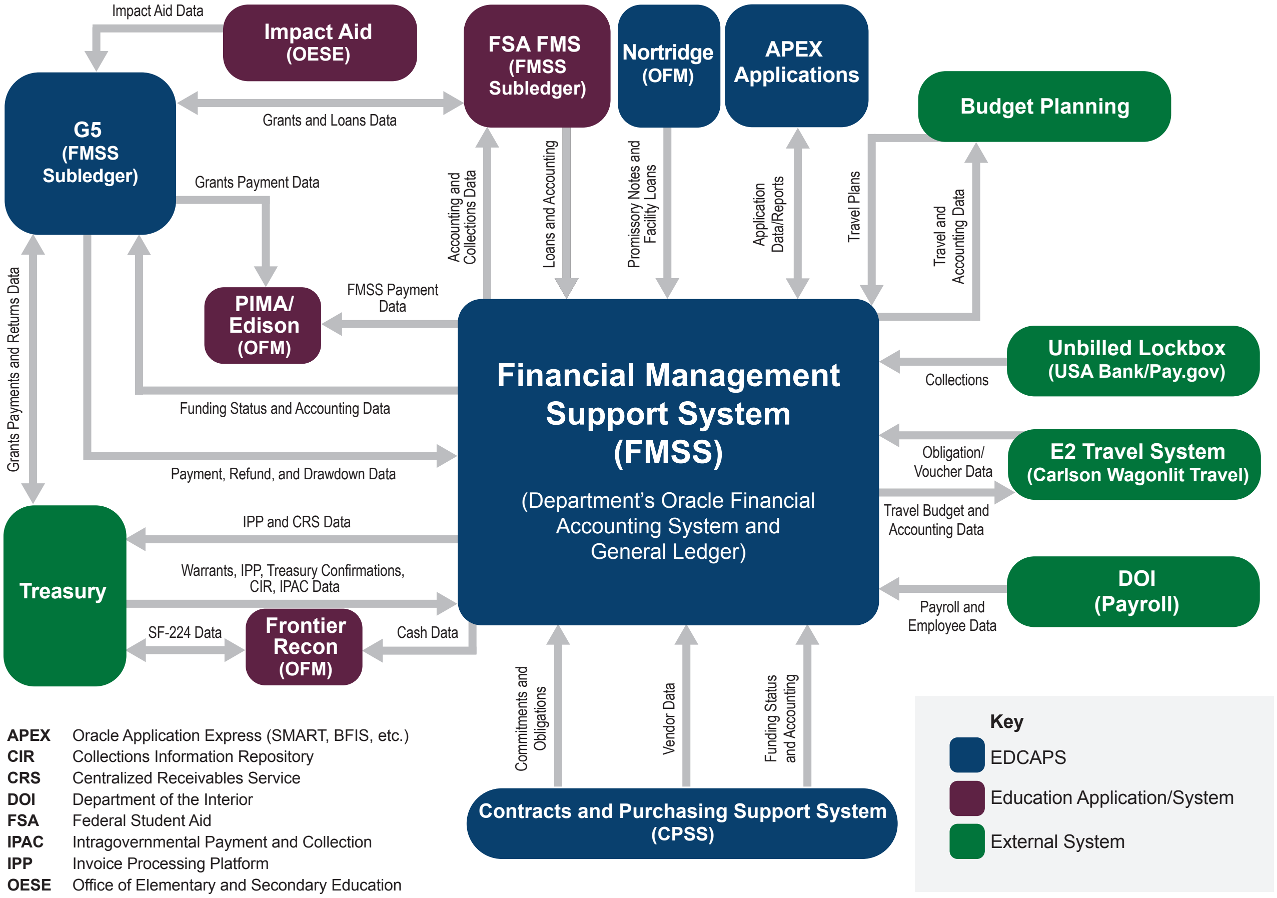
- General ledger—Preparation of financial statements and reconciliation of general ledger balances with subsystems maintained in program areas and Treasury.
- Funds management—Budget formulation, budget execution, and funds control.
- Grants pre- and post-award processing, including grant payment processing.
- 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 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


Impact Aid Data
Impact Aid (OESE)
FSA FMS (FMSS Subledger)
Nortridge (OFM)
APEX Applications
Budget Planning
G5 (FMSS Subledger)
Grants and Loans Data
Grants Payment Data
Accounting and Collections Data
Loans and Accounting
Promissory Notes and Facility Loans
Application Data/Reports
Travel Plans
Travel and Accounting Data
Grants Payments and Returns Data
PIMA/ Edison (OFM)
FMSS Payment Data
Financial Management Support System (FMSS)
(Department's Oracle Financial Accounting System and General Ledger)
Unbilled Lockbox (USA Bank/Pay.gov)
Collections
Funding Status and Accounting Data
Payment, Refund, and Drawdown Data
Obligation/ Voucher Data
E2 Travel System (Carlson Wagonlit Travel)
Travel Budget and Accounting Data
IPP and CRS Data
Treasury
Warrants, IPP, Treasury Confirmations, CIR, IPAC Data
DOI (Payroll)
Payroll and Employee Data
SF-224 Data
Frontier Recon (OFM)
Cash Data
Commitments and Obligations
Vendor Data
Funding Status and Accounting
Contracts and Purchasing Support System (CPSS)
Key
EDCAPS
Education Application/System
External System

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 approximately 2,800 Departmental internal users in Washington, D.C. and 10 regional offices throughout the United States and territories. EDCAPS is serving approximately 40,970 external users, mostly users of Grants Management System (G5). In FY 2022, the Department conducted an annual risk assessment of EDCAPS and tested 103 IT security controls out of a baseline of 630 IT security controls, as follows:

- EDCAPS—18[3]
- FMSS—28
- CPSS—12
- G5—33
- E2—12

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 2022:

- 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 external systems:

[3] Number of IT controls tested. No significant deficiencies or material weaknesses were identified.

- 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, CRS invoices, warrants, Treasury confirmations, CIR collections and administrative return, collections/payments).
  - Department of Interior systems (Payroll).
  - 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. 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:

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,[4] 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 2021, the OIG concluded that the Department was not compliant with PIIA because it did not meet one of the six compliance requirements. Specifically, the Department reported an improper payment estimate for the Title I, Part A program of 14.77 percent. 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. The Department's improper payment estimates were not reliable for three of its programs (Title I, Part A; Pell; and Direct Loan) that required an estimate for FY 2021. Specifically, the improper payment sampling and estimation plan the Department developed for the Title I, Part A program was not adequate for State Educational Agencies (SEAs) that use an advance payment process that does not allow the SEA to directly link payment transactions (expenditures) to specific G5 system drawdowns.

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

Debt Collection Improvement Act of 1996 (DCIA)

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 *Digital Accountability and Transparency Act of 2014* (DATA Act), Pub. L. 113-101, 128 Stat. 1146, amended Section 3716(c)(6) of the DCIA to require notification of a legally enforceable nontax debt that is over 120 days delinquent to the Department of the Treasury for purposes of administrative offset. While the Department continued to work toward an accelerated process to refer delinquent debt to Treasury, extension of the provisions of the *Coronavirus Aid, Relief, and Economic Security Act* (CARES Act) in FY 2022 continued to afford administrative forbearance for eligible loans. Beginning in March 2020, the provisions of the CARES Act suspended involuntary collection through the Treasury Offset Program. The suspension of involuntary collections will continue to apply through 2023. Pursuant to the CARES Act and related authorities, no loans were required to be transferred to Treasury during FY 2022. Accordingly, the Department was and is compliant with DCIA as amended by the DATA Act.

[4] *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.*

Federal Information Security Modernization Act of 2014 (FISMA)

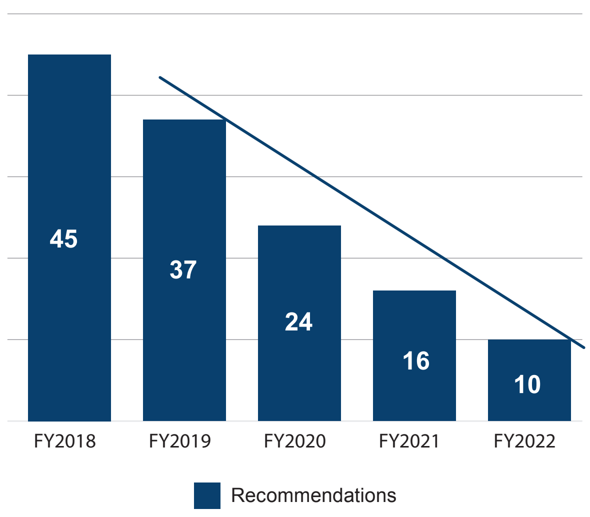
The ***Federal Information Security Modernization Act of 2014*** (FISMA 2014) requires federal agencies to develop, document, and implement an agencywide program to provide security for the information and relevant information technology systems. The Act supports the operations and assets of the agency 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 2022 to improve cybersecurity capabilities and functions, some of which include:

- The Department received an overall *Federal Information Security Modernization Act of 2014* (FISMA) assessment of "Effective," or a Level 4 Cybersecurity Maturity Level for FY 2022, which marks a significant improvement from FY 2021. This is the first time the Department has achieved this level with seven of nine FISMA domains increasing in score, as supported by information in the graphics below.

Security Function	Metric Domain	Maturity Level	Change from 2021	Met Federal Goal
Identify	Risk Management	Consistently Implemented	=	
Identify	Supply Chain Risk Management	Consistently Implemented	▲	
Protect	Configuration Management	Managed and Measurable	▲	✓
Protect	Identity and Access Management	Consistently Implemented	▲	
Protect	Data Protection and Privacy	Consistently Implemented	=	
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	▲	✓

FISMA Recommendations 2018–2022



- In February 2022, the Department implemented a new cybersecurity policy framework aligned with Executive Order (EO) 14028 Improving the Nation's Cybersecurity and ***National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5.*** The updated framework ensures a more comprehensive inventory of policies that directly align with the latest catalog of security control families and requirements levied through EO 14028. Five Instructions and 22 Standards have been converted into 20 new Standards (control families) aligned with the Cybersecurity Framework (CSF) and NIST 800-53, Revision 5. The framework modernizes the Department's cybersecurity policies, enables system stakeholders to find the Department's requirements quickly, and allows for updates to the Department's system of record for FISMA reporting, Cyber Security Assessment and Management System (CSAM) with ED-defined control parameters to support System Security Plan (SSP) development and assessments. This includes control overlays for requirements not within 800-53 control baselines, and enhances maintenance and strengthens the ability to update for new requirements while maintaining mapping to CSF rapidly and NIST controls.

- The Department released Standard PR.DS: Protection of Federal Tax Information. Released in January 2022, this standard establishes the Department standards for safeguarding the confidentiality of Federal Tax Information (FTI) as required by Internal Revenue Service (IRS) Safeguards Program 1 and IRS Publication 1075, Tax Information Security and Privacy Guidelines for Federal, State and Local Agencies. This is in accordance with Internal Revenue Code (IRC), Section 6103(p)(4)3; and IRS Publication 1075, as a condition of receiving FTI directly from either the IRS or from secondary sources.

- Office of the Chief Information Officer (OCIO) refined and used the Department's cybersecurity risk tolerance and appetite, which integrates with the Department's overall ERM program. In FY 2022, OCIO updated its target profile and key performance indicators (KPI) and key risk indicators (KRI) to support tracking and reporting progress made towards the Department's OCIO ERM target profile. OCIO continues membership and participation in ERM Working Groups and mini working groups (ERMWG) to continue to mature integration of Cyber Risk Management with ERM:
    - ERM maturity model metric refinement.
    - ERM digital tools risk reporting and analysis.
    - ERM training for leaders and staff.
    - ERM knowledge management.
- The Department's Security Assessment Team worked with OCIO to implement the Ongoing Security Assessment & Authorization (OSA) program, which started in December 2021. The OSA program and method of assessment replaced the older static-point-in-time assessment model of Assessment & Authorization. The threshold for entry into the OSA program is a risk assessment that focuses on the following areas: system demonstration, control baseline and inheritance review, and the Department's CSF Scorecard and discrepancy reports. The OSA program will reduce steps and modify artifacts to improve efficiency. The overall outcome is more frequent system stakeholder engagement and timely risk visibility.
- OCIO publishes monthly Department's CSF Risk Scorecards as part of the Department's Information Security Continuous Monitoring efforts to identify cybersecurity risks, issues, and opportunities for improvements in its 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 2022, the Department continued to mature its risk management processes through enhancements made to the CSF Risk Scorecard. These enhancements have improved the accuracy and timeliness of the Department's risk reporting and continuous monitoring. System stakeholders are now provided daily visibility of their system's risk and data quality. Additional views were established to augment and consolidate risk reporting to allow the Department's authorizing officials to quickly identify which systems require attention and prioritization of authorization and risk reduction activities. These enhancements are targeted to result in a reduced number of past due Plan of Actions and Milestones (POA&M) and data quality issues. With near-real time risk scoring and reporting in place, executive and system level stakeholders can effectively prioritize and manage the Department's cybersecurity risk daily.
- Throughout the year, the Department continued outreach and risk communications by disseminating monthly "State of IT" reports to the Department's senior leaders. These executive-level reports provide the Department's senior leaders with a holistic view of their IT investments, services, and cybersecurity posture through comprehensive IT and cybersecurity trends, metrics, and key insights to prompt top-down engagement and actions. These reports prepare senior POC leaders for the Monthly Deputy Secretary cybersecurity briefings facilitated by the Department's Chief Information Security Officer (CISO). The meeting communicates Department cyber risks, trends, metrics, key insights, upcoming announcements, and actions.
- The Department continued to mature its risk management processes through enhancements to the CSF Risk Scorecard. POC leadership can now monitor status of program-level business continuity planning and testing activities. These enhancements allowed the Department to close corrective action plan (CAP) 8.3 from the FY 2020 FISMA audit and are targeted to result in consistent implementation of business continuity planning activities. In FY 2022 Quarter 1, the Department enhanced its Power BI reporting to track and report compliance with the Department's 14028 mandates including, but not limited to, Multifactor Authentication (MFA), encryption, and resiliency. The FISMA Dashboard was also enhanced to visualize compliance statuses against recently released FY 2022 OCIO Metrics reporting guidelines (v1.1), issued by OMB/Cybersecurity and Infrastructure Security Agency (CISA) in support of EO 14028 requirements.

- In FY 2022, the Department was approached to provide a demonstration of its cybersecurity risk scoring and visualization capabilities to several partner federal Departments. As a result of the Department's demonstration of risk scoring and visualization capabilities, the partner Departments have expressed interest in establishing similar capabilities within their cybersecurity mission space.

- The Department established a Vulnerability Disclosure Policy (VDP) program in FY 2021, to provide an open channel and legal safe harbor for the discoverer of vulnerabilities to report it to the Department. The VDP allows the research community and others to alert the Department about vulnerabilities in its systems through a clearly established program. The Department expanded the VDP program in FY 2022 Quarter 1 to cover all internet accessible Department systems. Information submitted to the Department under the VDP will be used to mitigate or remediate internet-accessible systems and services vulnerabilities, or vendors' internet-accessible systems or services.

- The Department updated internal vulnerability management procedures in accordance with Binding Operational Directive (BOD) 22-01 Reducing the Significant Risk of Known Exploited Vulnerabilities. The Department continues to remediate each vulnerability according to the timelines set forth in the CISA-managed vulnerability catalog. The Department is working with CISA to mature Continuous Diagnostics and Mitigation (CDM) capabilities to augment and enhance remediation actions as required by this directive.

- The Department developed and implemented a new FISMA 2014 reporting dashboard through Microsoft Power BI to reflect the updated FY 2022 OCIO Metrics. The new dashboard allows leadership to visualize all data collected across the Department in support of its quarterly reporting requirements to DHS and OMB. The dashboard provides the ability to proactively identify discrepancies or potential risks as a result of data captured and presented to both leadership and FISMA 2014 metric owners for action.

- The Department took immediate action in Quarter 1 and Quarter 2 regarding M-22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles by creating, funding, and onboarding a GS-15 zero-trust architecture (ZTA) program manager and releasing a Department strategy and project schedule for full implementation by the end of FY 2024. The Department received the initial transfer of $15 million in Technology Modernization Fund (TMF) funds, used to:
    - establish a ZTA Project Management office (PMO).
    - engage the recompete of Enterprise Identity, Credential, and Access Management (ICAM).
    - obtain Secure Access Service Edge (SASE) & Security Orchestration Automation & Response (SOAR) capabilities.

There is ongoing collaboration between ZTA, ICAM, Enterprise Detection and Response (EDR), and Cyber Data Lake (CDL) PMOs to fulfill progress towards all pillars of Zero Trust. A "zero trust" approach to security provides the Department with a necessary and defensible architecture against increasingly sophisticated cyber-attacks. The Department is on track to meet the requirements set forth by OMB and maintain a resilient cybersecurity posture.

- During the first half of FY 2022, OCIO successfully continued to provide IT services to support nearly 100% telework in response to the COVID-19 pandemic. However, during the second half of FY 2022, the Department shifted from nearly 100% telework to a hybrid telework posture. Throughout this transition, there was no significant impact or compromise to the Department Information Security Program, and the Department continued execution of missions without interruption. Despite the challenging work environment necessitated by the COVD-19 pandemic and the evolving technology changes to meet working requirements, the Department did not have any major information security incidents occur. To continue strengthening its cloud portfolio, the Department has continued its close working relationship with the FedRAMP Project Management Office (PMO) which established increased reoccurring continuous monitoring meetings with participating agencies to help improve the security posture of those Cloud Service Providers.

- In response to the January 2022 Apache Log4j vulnerability, the Department Vulnerability Management (VM) team identified all impacted systems, assets, and remediation actions. All reports were forwarded to the EDSOC for further incident response activities. The EDSOC coordinated across the Department (FSA Security Operations Center [SOC], CSOC, etc.) to identify impacted assets, patch immediately, block indicators of compromise, and take necessary incident response actions if compromises were discovered. The EDSOC completed all network traffic and forensics analysis on the Department's systems and concluded that no Department assets showed indication of a successful compromise. The Department was selected to participate in the first Cybersecurity Safety Review Board analysis of Log4j and was cited as providing the most input and support of Federal Cabinet-level Departments.

- In response to Emergency Directive 22-03 Mitigate VMWare Vulnerabilities, the Department issued a CISO Memorandum on May 20, 2022. Information System Owners and Information System Security Officers were required to enumerate all instances of impacted VMWare products within their system authorization boundaries, report findings to the OCIO VM team, and deploy updates (or remove the VMWare product until an update is available). There were no findings of impact to the Department, which was reported to CISA.
- The Department implemented measures in the wake of the COVID-19 pandemic to permit remote work, including issuance of Standard PR.AC: Emergency personal identity verification (PIV) Alternative Standard. As restrictions have been lifted and per the requirement of Homeland Security Presidential Directive 12, the Department released a CISO memorandum on April 15, 2022, for the rescission of Standard PR.AC. As a result of the memo, more than 90% of Department users are now utilizing PIV. This ensures the security of user access to the Department's networks and systems.
- In support of SOC consolidation and maturation, the Department continues to identify task separation, integrate security tooling, coordinate incident investigation and response, and remove duplication between the Department's two SOCs, EDSOC and FSA SOC. Existing milestones include refining current processes that support incident response and management to be aligned to a singular source, establishing automation within our incident response tool, and evolving training on newly enhanced processes and technologies. In FY 2021, the SOC maturation plan was updated to address key requirements levied on the Department in support of the recently released EO 14028 on Improving the Nation's Cybersecurity and NIST 800-53 Revision 5. Updates to the plan in FY 2022 will result in improved incident response (IR) maturation in keeping within Federal IR requirements, continued improvement to our data loss prevention systems, increased cost savings through virtualization, and increased use of specialized personnel dedicated to threat intelligence analysis, law enforcement cooperation, and hunt team activities, providing a more robust and complete threat analysis product to our customer.