Analysis of Systems, Controls, and Legal Compliance

MANAGEMENT ASSURANCES

The Secretary of the Department of Education's Fiscal Year 2021 Statement of Assurance provided below is the final report produced by the Department's annual assurance process.

STATEMENT OF ASSURANCE
FISCAL YEAR 2021
November 19, 2021

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 (DQP) in accordance with Appendix A of OMB Circular A-123.

With the exception of a material weakness in financial reporting in the Independent Auditors' Report, the Department has not identified any material weaknesses in internal controls: operations, reporting, or compliance with applicable laws and regulations. The Department considers the applicable internal controls to be working effectively.

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, 2021.

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 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.

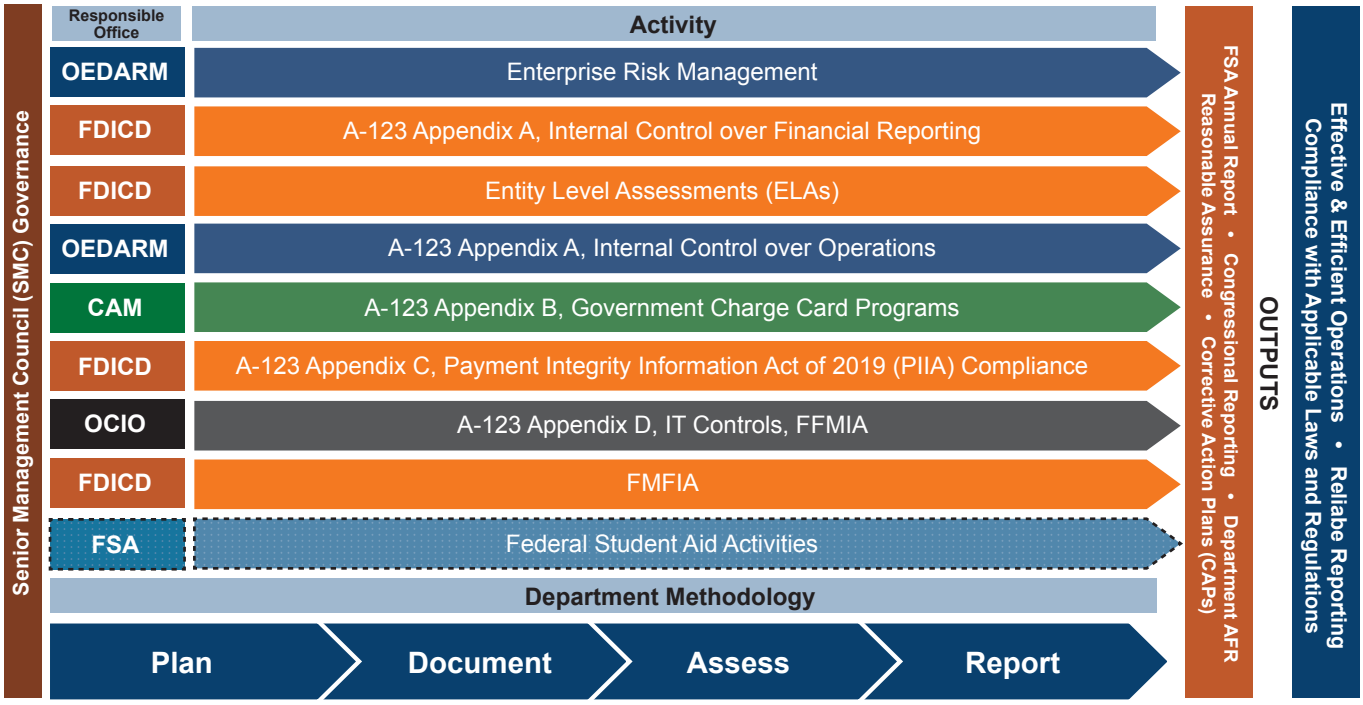
This section describes the Department's internal control framework, offers an analysis of the effectiveness of its internal controls, and explains assurances provided by the Department's leadership that internal controls were in place and working as intended during FY 2021 to meet the three objectives.

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



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 compliance process oversight and more informed monitoring of internal controls and risk management by all offices and governance bodies, including the Department's Senior Management Council. This framework also allows for the Department to obtain the outcomes of a better control system and a reduced risk landscape. Furthermore, this streamlined approach helps the Department provide reasonable assurance to internal and external stakeholders that the data produced by the Department is complete, accurate, and reliable; 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 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 2021, the Department and 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, 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 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 DQP 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, 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.

In FY 2021, the Department tested a proportionate number of key financial controls for both grant and non-grant areas based on qualitative risk assessments and rotational test plans. 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, such as verifying immaterial differences, obtaining electronic signatures, and updating policies and procedures.

ANALYSIS OF FINANCIAL MANAGEMENT SYSTEMS

The FFMIA requires management to ensure that the Department's financial management systems consistently provide reliable data that comply with federal financial management system requirements, applicable federal accounting standards, and the U.S. Standard General Ledger at the transaction level. Appendix D to OMB Circular A-123, Compliance with the 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.
- 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 40,970 external users, mostly users of the G5. In FY 2021, the Department conducted an annual risk assessment of EDCAPS and tested 104 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 2021:

- 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:

- Department Systems:
  - Oracle Enterprise Performance Management Cloud Planning (formerly Hyperion).
  - Frontier.

- G5 Grants
- CPSS Contracts Purchasing Support

- 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 admin 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[1], 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 AFR and accompanying materials, and to determine whether the agency has met six compliance requirements.

In its annual improper payment compliance audit for FY 2020, the OIG concluded that the Department was not compliant with PIIA because it did not meet two of the six compliance requirements, as described in Finding 1. Specifically, the Department did not demonstrate improvement in reducing improper payments in the William D. Ford Federal Direct Loan (Direct Loan) Program. In addition, the Department reported improper payment rates that exceed 10 percent for the Temporary Emergency Impact Aid for Displaced Students (Emergency Impact Aid) and Immediate Aid to Restart School Operations (Restart) programs.

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

Debt Collection Improvement Act of 1996

The *Debt Collection Improvement Act of 1996 (DCIA),* **Pub. L. 104-134**, 110 Stat. 1321-358, was enacted into law as part of the *Omnibus Consolidated Rescissions and Appropriations Act of 1996*, **Pub. L. 104-134**, 110 Stat. 1321. The primary purpose of the DCIA is to increase the collection of nontax debts owed to the federal government. Additionally, the *DATA Act*, **Pub. L. 113-101**, 128 Stat. 1146, amended Section 3716(c)(6) of the DCIA to require notification of a legally enforceable nontax debt that is over 120 days delinquent to the Department of the Treasury for purposes of administrative offset.

Due to unique program requirements of the *Higher Education Act of 1965* (HEA), in 2015 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 the 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 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, 2021, FSA's current business process requires loans to

[1] *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.

be transferred to the default loan servicer after 360 days of delinquency. FSA refers debt to TOP after exhausting due process with each borrower, which extends beyond the delinquency period in the DATA Act. Further, due to the number of entities and systems involved in handling student loan debts and the decentralized nature of such processes, FSA is not yet capable of meeting an accelerated time line. Accelerating the timeline requires substantial changes to servicing legacy systems. Rather than making changes to these legacy systems, FSA plans to build new TOP referral requirements into the NextGen FSA servicing platform. FSA has developed a long-term project plan to incorporate the referral requirements into servicer contracts and guaranty agency agreements to initiate the required system programming changes. This determination that the Department does not have a process in place to enable the referral of FSA owned Title IV debts on the 271st day of delinquency and referral of relevant FFEL claims and delinquent Perkins Loan debt on the 121st day of delinquency does *not* represent a material weakness in the Department's internal controls.

While the Department continues to work on an accelerated process to refer debt to Treasury, the *Coronavirus Aid, Relief, and Economic Security Act* (CARES Act) affords administrative forbearance for eligible loans. Beginning in March 2020 and continuing throughout FY 2021, the CARES Act suspended involuntary collection through TOP. This suspension of involuntary collections will continue to apply at least through January 31, 2022. Pursuant to the CARES Act and related authorities, no loans were required to be transferred to Treasury during FY 2021. Accordingly, the Department was and is compliant with DCIA as amended by the DATA Act.

Federal Information Security Modernization Act of 2014

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 information systems that support the operations and assets of the agency and to ensure the confidentiality, integrity, and availability of system-related information.

The Department's and FSA's information security programs completed numerous significant activities in FY 2021 to improve cybersecurity capabilities and functions, some of which include:

- 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 enterprise risk management (ERM) program. Key performance indicators (KPI) and key risk indicators (KRI) have been established 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.

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 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 2021, 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.

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.

OCIO established initial operating capabilities for the Department's cybersecurity data lake and continued to enhance configuration for ingestion of Continuous Diagnostics and Mitigation and continuous monitoring data. Currently, 10 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 Alternative Solution (PIV-A) as an alternative multifactor 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 virtual private network (VPN) capacity supporting the workforce during the 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 using a 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 capability for nongovernment-furnished equipment within the Department's new IT environment that is superior to capabilities that existed before 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 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 2021, the Department's DLP solution identified and blocked 9,562 emails which prevented potential sensitive personally identifiable information security incidents.
- Through enhanced reporting of email and web security posture, the Department was able to maintain U.S. Department of Homeland Security (DHS) Binding Operational Directive (BOD) 18-01 compliance of 100 percent for email security and 97 percent for Hypertext Transfer Protocol Secure (HTTPS) tracking. Additionally, there were no overdue critical or high vulnerabilities in FY 2021 for the Department'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.
- OCIO continued conducting quarterly Department-level, system-tailored Incident Response and Contingency Plan testing tabletop exercises virtually, which focused on contingency planning in the event of a cyber incident. As of September 2021, 98 percent of the Department's FISMA 2014-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.
- 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 in a position related to cybersecurity. In July 2021, the Department spoke to students from SFS about the Department's internship and upcoming employment opportunities
- OCIO established a roadmap for migrating the Department's policies and security control

implementation from National Institute of Standards and Technology SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 4 to Revision 5. This road map will allow the Department to better understand, plan, and prepare as it begins to update key security controls in accordance with the new Revision 5 guidance. The Department also participated in a cross-agency working group with GSA, HHS, and other agencies to collaborate on the development and standardization of organizational parameters for the NIST 800-53 Revision 5 security controls.

- OCIO has implemented an ACS Directive, OCIO: 3-114, *Cybersecurity Awareness Simulated Phishing Exercise Behavioral Based Escalations*, which establishes the Department standards for acceptable behaviors in response to an authorized simulated phishing exercise as well as behavioral-based escalations for federal employees and contractors based upon identification of a pattern of unacceptable behaviors (e.g., repeat-risk email users) that puts the network and data at risk. This directive also documents actions required to reduce Departmental risk from end users who exhibit unacceptable behaviors in response to one or more exercise(s). In support of this new directive, OCIO established enhanced reporting and retraining support for privileged users and repeat risk users. All privileged users who had unacceptable behavior as a result of the first exercise conducted, were required to and have completed the necessary training courses.
- OCIO supported all required actions from DHS Emergency Directive 21-01, *Mitigate SolarWinds Orion Code Compromise*. The Department immediately disconnected/powered down SolarWinds Orion products, versions 2019.4 through 2020.2.1 HF1, from the Department network and notified the Cybersecurity and Infrastructure Security Agency (CISA) on December 14, 2020, as required. The Department continues to analyze forensic images of system memory and/or host operating systems for all impacted assets. OCIO completed a forensics analysis and an independent, external, third-party, certified forensics examiner determined no threat actor was present in the system and no malicious activity has taken place. Additionally, OCIO also provided both the Senate and U.S. House of Representatives formal responses to inquiries regarding this emergency directive.
- OCIO supported all required actions from DHS Emergency Directive 21-02, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*. The Department immediately disconnected impacted exchange servers from the Department's network and notified CISA on March 5, 2021. All impacted assets were updated to the latest version required by CISA by March 9, 2021.
- The Department, including the FSA Zero Trust strategic implementation plan, addresses current issues with access, including unauthorized, and siloed single-point solutions for data protection. This initiative establishes an architectural plan; a solution design; an accompanying process; and implements a secure framework to address access, verification, and integration issues across all information systems hosted at multiple independent data centers and within numerous cloud service providers. The Department and FSA will leverage Zero Trust concepts to move to a data-centric access and protection model versus the traditional network-based perimeter protection concepts. The submitted plan outlines the development, modernization, and enhancement of the program:
  - Establish and fully implement a Zero Trust Program that includes strategy, architecture, design, and an implementation road map.
  - Develop Zero Trust workbooks and standards to support adaptation of Zero Trust for the Department.
  - Establish a catalog of Zero Trust services and capabilities.
  - Adopt Zero Trust across cloud-computing environments in accordance with the developed road map.
  - Establish a Zero Trust-specific section in the cybersecurity training program.
  - Adopt multifactor authentication and encryption for data at rest and in transit, to the maximum extent consistent with federal records laws and other applicable laws.
- To mitigate impacts of the COVID-19 pandemic on remote stakeholders, the Department identified, analyzed, and implemented a cloud-based solution to provide rapid expansion of the Department's VPN capacity to support extensive teleworking capabilities. As a result of these efforts, the Department was able improve the availability and continuity of operations

for its networks. The Department also provided targeted outreach to proactively address threats to teleworking employees (e.g., warning them of increased phishing attempts and other cybercriminal scams that target largely at-home workers). As a result of this increased outreach, the Department has benefitted from an improved average reporting rate (+7 percent) for its phishing exercises across its user base in FY 2021 from FY 2020.

- The Department issued an amendment to Acquisition Alert (AA) 2020-01, *Education Acquisition Regulation (EDAR) Class Deviation: Cyber and Personnel Security Requirements for Contractors*. This amendment implements deviated EDAR clauses to accurately reflect the Department's updated cybersecurity and privacy requirements. Below are the requirements added/updated:
  - DHS Binding Operation Directives.
  - Continuous Monitoring / Ongoing Security Assessment & Authorization.
  - Identity, Credential, and Access Management and Personal Identify Verification (PIV) Systems.
  - National Institute of Standards and Technology (NIST) Zero Trust Architecture/Zero Trust Network.
  - Department Cyber Data Lake.
  - Office of Management and Budget (OMB) Trusted Internet Connections 3.0.
  - *National Defense Authorization Act* Section 889 Compliance.
- The Department's cybersecurity risk exposure has been directly reduced due to the amendment to this alert that allows the Department to enforce all the newly updated cybersecurity requirements articulated in the revised cybersecurity clause (which became effective September 28, 2020) with the amendment to Acquisition Alert 2020-01. The OCIO Information Assurance Services Division reviews all new IT contracts as a part of the ERM review process ensuring the updated clause inclusion before contract award.
- To allow the research community and others to alert the Department about vulnerabilities in its systems through a clearly established program, the Department *Vulnerability Disclosure Policy* (VDP) was published on March 1, 2021, in accordance with DHS BOD 20-01. The Department's VDP provides an open channel and legal safe harbor for the discoverer of vulnerabilities to report them to the Department. Version 2.0 of the VDP, released June 1, 2021, expanded the scope of the policy to include all internet-accessible, public-facing systems or services of the Department, more than a year ahead of schedule.
- Leveraging lessons learned with the Department of Energy, the Department formally established an Information Communications Technology (ICT) Supply Chain Risk Management (SCRM) program and released a strategic road map designed to provide a vision and action plan for the planning, preparation, implementation, and execution of the Department's ICT SCRM program. Following this road map and plan will allow the Department to move from a point-in-time compliance model to a near real-time detection, analysis, and correction model, resulting in improved ICT SCRM and more accurate and frequent assessments of ICT SCRM security control effectiveness. The Department's ICT SCRM program ensures that the Department and its contractors are assessing, protecting, and measuring risks involved with their selection of suppliers and not accepting unnecessary risks.
- The Oracle Enclave has been created for integrating all Oracle license usage into one cluster for cost avoidance. An approximate $7 million in savings is estimated for the Department over three years, beginning in 2022. Currently, the Department is using this enclave for several systems, including EDCAPS, ED*Facts*, and PIVOT-I.
- OCIO, via the Information Technology Program Services Division, recently activated the Technology Business Management Solutions (TMBS) to provide cost transparency through a single, integrated view of IT costs by service, office, line item, and project. TBMS will empower Department leaders with information to improve financial performance.
- During FY 2021, OCIO successfully completed a major infrastructure upgrade in the Department's disaster recovery environment in Raleigh, NC. Enterprise improvements included an increase to overall infrastructure performance, dependability, capacity, and security. This upgrade provides the Department with a significant increase to the network bandwidth from 10GB to 40GB, increased cloud computing resources (the number of hosts increased

by 30 percent, RAM by 100 percent, and cores by 25 percent) resulting in overall improved performance, resolution of several existing vulnerabilities and POA&Ms that enhance the security posture of the Raleigh datacenter.

- OCIO implemented a Human Capital, Financial and Resource Management tool, comprised of a suite of dashboards, that provides an on-demand, interactive, and consolidated view of critical management areas. The tool is designed with a primary focus on providing executive-level status views of human capital management, financial management, budgetary execution and procurement to OCIO's senior leadership and leaders at the division and branch levels. The critical data points that leaders need to make informed business decisions are updated throughout the day to ensure that OCIO is proactively able to meets its strategic objectives and goals. These unique dashboards are discussed below:
  - The Human Resources Hiring Dashboard provides leadership with an up-to-the-minute aggregate or divisional snapshot view reflecting the status of current hiring actions. It lists the number of positions that have received agency approval to be encumbered, the number of positions presently encumbered, hiring actions that are not yet complete, and the number of new hires that have begun their employment with OCIO during the current fiscal year. In addition, updates are incorporated to identify the stage of each hiring action within the recruitment process. The Office of Human Resources has created a service-level agreement (SLA) identifying the number of days for each phase of the recruitment process in alignment with the OPM's 80-day hiring model. Those time lines are listed within the dashboard along with averaged quarterly variances that have occurred. In addition, current actions where SLAs have been missed are labeled as such, and viewers are able to specifically see the exact SLAs that have deviated from the prescribed time lines.
  - The Central Information Technology (CIT)-focused dashboard improves financial transparency and accountability for OCIO's leadership, division branch chiefs and program/project managers by increasing visibility into quantitative and qualitative key metrics. The key metrics reported include annual allocations, allotments, year-to-date-spending for both CIT and non-CIT budget line items, as well as late Acquisition Plan (AP) actions. Division chiefs and programs can visually and quickly identify areas that require their attention, such as projects still having the most remaining funding, late AP actions, and AP actions due in 30/60/90 days. Divisions are then held accountable for executing their plans accordingly.
  - The non-CIT dashboard focuses on pay and nonpay budgets and has been essential in driving critical decisions throughout the year, including pay and training availability for OCIO's employees.
  - While the OCIO Financial Executive Dashboard was primarily developed with the executive leadership audience in mind, it has served a multifaceted purpose as the basis for numerous tactical actions at the next level of leadership in both CIT and non-CIT.
- OCIO launched standard operating procedures for the proper alignment and retention of records inventories. These procedures enable principal offices to strengthen the protection of controlled unclassified information.
- In FY 2021, the Department's High Value Asset (HVA) program, in partnership with FSA, was presented as a "Best in Government" for its engagement with the DHS assessment team. DHS senior leadership noted how the Department and its components were outstanding in their planning, coordination, execution, and timeliness of its Risk and Vulnerability Assessments. Highlights of the program expressed how the Department worked with DHS to ensure a seamless process was executed for HVA assessment. This was presented at the federal CISO Council HVA Subcommittee as the gold standard for HVA engagement.

- In FY 2021, the Department's Cybersecurity and Awareness Program Manager was awarded the 2021 Federal Information Security Educators Cybersecurity Awareness and Training Innovator Award. The Department Cybersecurity and Awareness Program Manager oversees the Department's Phishing Program, Cybersecurity and Privacy Awareness Training, Role-Based Training, Workforce Development, and Continuous Outreach Activities.
- The Department developed and implemented a new FISMA 2014 reporting dashboard through Microsoft Power BI. 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 first quarter submission provided favorable Risk Management Assessment results across all FISMA 2014 security domains.