U.S. Department of Education

Office of the Chief Information Officer

Information Resources Management Strategic Plan

FY 2022 – FY 2026

December 2, 2021

Table of Contents

Introduction

The US Department of Education's (ED or Department) mission is to ***promote student academic achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access***. ED's ability to provide world-class technology services to its employees and stakeholders nationwide is critical to achieving this mission. The Information Resource Management (IRM) Strategic Plan sets forth the Chief Information Officer's (CIO's) vision for using information technology (IT) to support ED's mission while protecting the public's right of access to Department information. This plan describes the strategic goals necessary to achieve the CIO's vision. The goals and objectives outlined in the IRM Strategic Plan will guide the IT modernization efforts needed to transform the Department.

The IRM Strategic Plan outlines the work needed to improve ED's IT governance, deliver reliable, mission-focused IT solutions, strengthen cybersecurity capabilities, and engage, train, and communicate with staff about IT across the Department. The IRM Strategic Plan aligns with and supports the Department's Strategic Plan, the President's Management Agenda (PMA), Cross Agency Priority (CAP) goals related to Federal IT initiatives, and ED's Data Strategic Plan.

Overall, the IRM Strategic Plan highlights the Department's ambitious transformation journey from Fiscal Year (FY) 2022 to FY 2026 to improve overall IT service delivery, enhance ED's IT performance management practices, and increase protection of government systems and the data within.

About the IRM

Purpose

Establish how the Department will use information management resources to support its mission over a four-year time span. The IRM Strategic Plan supports ED's Strategic Plan and details the goals and objectives needed to effectively prioritize and manage ED's IT portfolio.

Mission

Support the Department of Education's mission through the acquisition and effective management of technology.

Goals

1. **Strengthen the Department's IT Governance |** Ensure the Department manages IT investments through their lifecycle – from initiation to retirement – and fosters transparency across the IT portfolio to support ED's mission.
2. **Deliver Reliable, Mission-Focused IT Solutions |** Strive to meet or exceed external and internal customer expectations and needs in various settings by acquiring and deploying reliable technology solutions.
3. **Enhance the Department's Cybersecurity Capabilities |** Strengthen ED's ability to protect and safeguard the personal and financial data housed within its systems, optimize ED's risk posture, and mature the Department's ability to identify, protect, detect, respond, and recover from cybersecurity threats.
4. **Improve the Department's IT Communications and Engagement |** Ensure that Department staff are aware of IT resources and requirements through outreach, engagement activities, and effective IT communications and that IT staff have the tools, training, and support they need to meet ED's mission.

Authority

The IRM Strategic Plan integrates external policies and directions as defined by Congress and the Administration including:

- Clinger-Cohen Act of 1996
- Federal Information Technology Acquisition Reform Act (FITARA) of 2014
- OMB, Revised Circular A-130
- Federal Records Act of 1950
- 36 Code of Federal Regulations (CFR) B – Records Management
- OMB/National Archives and Records Administration (NARA) Transition to Electronic Records Directive (M-21-19)
- Rehabilitation Act of 1973, Sections 504 and 508
- Executive Order 13556 – Controlled Unclassified Information (CUI)
- 36 Code of Federal Regulations (CFR) B – Controlled Unclassified Information (CUI)
- Federal Information Security Modernization Act of 2014
- Foundations for Evidence-Based Policymaking Act of 2018 (Evidence Act)
- 21st Century Integrated Digital Experience Act (21st Century IDEA)

Role of the Chief Information Officer

As the Department's executive agent for IT resources, the CIO works across organizational Principal Office Components (POCs) in planning and evaluating technology needs and providing advice and assistance to the Secretary of Education on the acquisition and management of information resources. Specifically, the CIO works with ED's Senior Leadership to develop a shared vision for conducting and optimizing ED's IT business processes. The CIO also sets policies to manage information resources effectively, ensures value-added technologies are available to fulfill agency needs, and provides IT services to ED POCs.

Execution

Execution of the IRM is subject to the final approval of implementation plans and the availability of funding and other resources. The Department may need to re-prioritize activities based on internal or external factors.

Strategic Goal 1

Strengthen the Department's IT Governance

Goal Leader: Director, Information Technology Program Services

Goal Overview

Effective IT governance depends on a strong Enterprise Architecture (EA), implementation of an IT governance framework to ensure unity in Information Technology Investment Management (ITIM) functions, and the effective distribution of, and training around, governance policies. A governance framework offers stakeholders transparency into requirements and regulations, which improves the effectiveness and efficiency of the Department's IT portfolio. This goal incorporates the work needed to facilitate ED's IT oversight and increase resource procurement and lifecycle management rigor.

The Department's IT governance framework is cross-functional and integrates capital planning, lifecycle management of IT investments and projects, and EA and requires the cooperation and engagement of cross-agency governance bodies. This framework links operational processes related to budget, acquisition, and human resource management with IT management functions such as operations management, cybersecurity, and privacy to ensure that the Department seamlessly plans for and controls IT investments, acquisitions, policies, and information management.

Anticipated Outcome

The Department has a modern IT governance framework that drives decisions on acquiring and integrating emerging technologies to save money, upholds FITARA through effective investment and project lifecycle management, and supports advanced information management governance capabilities to ensure access to people with disabilities.

Objective 1.1: Leverage the Department's Enterprise Architecture to Drive IT Modernization

A key component of effective IT governance is a well-documented, regularly updated EA available for Department staff to plan and implement IT modernization and performance improvement initiatives. Through this objective, ED will develop and launch an EA platform and associated processes, which will provide greater transparency and understanding of existing and future IT solutions across the Department. This objective supports effective IT planning and evaluation by improving transparency within the Department's EA repository, which will help Department staff's assessment of business needs. The automated EA will prevent the Department from duplicating existing technology solutions and promote shared service across ED.

The Department's current EA contains artifacts that describe the business processes, information and data flow, and IT systems and technologies included in the IT portfolio. ED will integrate EA into IT planning activities by defining ED's current and desired future state and identifying investments and transition activities required to move from present to future state.

Anticipated Outcome

The Department uses an automated EA repository populated with artifacts and information derived from an EA Modernization Planning Process to support IT decision making.

Objective 1.2: Improve Investment Lifecycle Management and Oversight for the Department's IT Portfolio

The Department will mature the IT governance framework by developing cross-functional IT governance boards to improve oversight, increase the efficient acquisition and use of IT, and promote standardized investment and project management practices. Increasing oversight and improving reporting about the IT portfolio will allow ED to optimize acquisition strategies, reduce the use of redundant or inefficient IT systems and services, and ensure that ED's IT spending is transparent and strategic. As part of the enhanced IT governance framework, the Department will implement standard evaluation criteria for IT investments or projects, which will improve ED's ability to conduct performance evaluations of IT assets. The Department will also establish a consistent, repeatable, and systematic process for assessing risks of all IT investments to ensure that risk ratings accurately reflect an investment's ability to accomplish its intended purpose.

The Department will mature the standard approach for planning, managing, and governing IT project delivery through the lifecycle management process by developing a comprehensive guide for IT program and project management. This approach will promote a multi-disciplinary review of IT projects to deliver IT systems or services cost-effectively. Last, this objective includes implementing and maturing Technology Business Management (TBM), which will integrate ED's IT budget and spending to improve IT cost transparency and insight into the factors that drive IT costs. Implementation of TBM will also provide decision-makers with the information needed to optimize the Department's IT footprint by retiring legacy platforms, accurately evaluating the ongoing costs of maintaining an IT system, and better identifying modernization opportunities.

Anticipated Outcome
The lifecycle management and IT portfolio and investment management processes and procedures are widely understood and followed across the Department, uphold FITARA, provide cost transparency, reduce overlap and duplication, and ensure that IT projects are performing as expected.

Objective 1.3: Automate Enterprise Information Management (IM) Capabilities

An essential part of IT governance is ensuring that Department staff understand their responsibility for managing the information they collect, produce, and disseminate. This work includes appropriately classifying and storing all records and making information accessible internally and externally to individuals with disabilities. Doing so ensures that ED meets statutory requirements, and that the Department's information is effectively and efficiently managed and readily accessible to those who need it.

ED will establish a paperless working environment that aligns with OMB directive M-19-21: Transition to Electronic Records, implements EO 13566 Controlled Unclassified Information, and is compliant with Section 508 accessibility requirements of the Rehabilitation Act. This alignment will enable the Department to eliminate the need to print and file paper records, automate CUI markings, and improve ED's ability to ensure applications processing data are 508 compliant.

Anticipated Outcome
The Department has automated policies for traditional records management, information preservation, protection, accessibility, and retention.

Strategic Goal 2

Deliver Reliable, Mission-Focused IT Solutions

Goal Leader: Director, Enterprise Technology Services

Goal Overview

The Department relies on IT services to meet the mission of serving the nation's students, teachers, and communities. For agency staff to be most effective, ED needs new or enhanced IT solutions to support innovation. Equally important is that ED's IT systems operate efficiently, changes and updates are implemented effectively, and without disruption to services, customer issues are addressed quickly and professionally, and users understand how to use and operate available technology. IT services must be reliable and accessible to support ED's increasingly mobile workforce, as disruptions in IT service undermine ED's ability to serve stakeholders across the nation. This goal reflects the work needed to improve the quality and capability of IT solutions available for ED staff and the public and the continuous improvement efforts required to ensure that ED can remain responsive to all stakeholder's IT needs.

Anticipated Outcome

The Department has the technological flexibility and agility needed to address new and changing customer requirements and prioritizes how the agency provides IT service and engages in continuous improvement so that solutions address the real-time requirements of ED's customers.

Objective 2.1: Enhance the Department's Ability to Deliver IT Service to the Public

The Department's IT services are essential for the nation's public to access and interact with ED services and information. ED's external customers rely on the Department's systems to be effortlessly accessible, dependable, and secure. As technology evolves, the Department will continue to develop user-focused solutions intended to improve the accessibility and efficiency of agency services. This objective ensures that ED's core IT infrastructure and supporting business processes are modernized to reflect the Department's changing needs and position ED to fully execute and achieve the desired outcomes of ED's applications and programs.

Anticipated Outcome

The Department's public stakeholders can easily find information, data, and engage in self-service activities, which will improve information transparency and accessibility.

Objective 2.2: Improve the Efficiency and Effectiveness of IT Service Delivery

Department staff rely on desktop, printing, network, and telecommunication services to complete their work and communicate with colleagues and individuals across the nation. The Department needs technology services that are reliable, resilient, consistent, and accessible. The Department will implement new tools and processes to improve its IT service delivery timeliness, responsiveness, and efficiency through this objective. The planned initiatives include enhancing ED's self-serve customer service portal and expanding the IT service catalog. These initiatives will improve customer service, decrease the response time for customer service requests, allow department leaders direct access to IT service information, and improve ED's ability to monitor and track service delivery efforts.

This objective will also focus on improving the accessibility and usability of the Department's technology to support an increasingly mobile workforce. Mobile computing gives staff greater flexibilities and can improve overall productivity, allowing ED to leverage talent from all over the country while also enabling ED employees to be agile in response to agency needs. Critical components of this objective include rolling out virtual desktops, enabling compatibility and interoperability across multiple hardware devices,

and utilizing cloud services to make applications and software accessible from various devices across locations.

Anticipated Outcome
Customers are mobile, have access to the cutting-edge technology they need, and the Department's back-end infrastructure is efficient and secure.

Objective 2.3: Engage in Continuous Improvement to Proactively Assess Customer IT Needs

To ensure that the IT services at ED meet the needs of staff and customers, the Department will proactively gather customer feedback to guide future adjustments and capture changing staff technology requirements and ideas. The Department must engage customers and staff to ensure that staff have the tools, information, and access to the technology they need to meet the organization's goals. The work under this objective will establish processes to assess staff IT needs and verify that solutions meet identified needs.

Anticipated Outcome
The Department gives customers regular, systematic opportunities to provide feedback about IT services and uses that information to improve how the agency supports and engages IT customers.

Strategic Goal 3

Enhance the Department's Cybersecurity Capabilities

Goal Leader: Director, Information Assurance Services

Goal Overview

Cybersecurity is critical to the business and mission of the Department. A lack of focus and investment in cybersecurity can directly impact ED's ability to serve the public. Cyber threats and incidents disrupt day-to-day operations, which may require the additional burden of repairing affected systems and result in a financial or reputational loss. This goal will guide both short and long-term enhancement of ED's enterprise cybersecurity program. It will provide a roadmap to improve the Department's security posture and protect its systems, applications, infrastructure, and information from cybersecurity threats. To ensure that cybersecurity risks are known and managed across the agency, the Department will incorporate cybersecurity reviews in all phases of ED's IT governance framework.

Anticipated Outcome

The Department manages cybersecurity risks to protect data and assets from unauthorized access, modification, or distraction from services supporting the agency mission, improve business and continuity management, improve stakeholder confidence, and improve recovery times in the event of a breach.

Objective 3.1: Enhance Organizational Capacity to Manage Cybersecurity Risk.

Enhancing ED's policies, processes, standards, and guidelines around cybersecurity risk management is critical to growing and improving ED's cybersecurity capabilities. The Department will formalize ED's cybersecurity risk management governance by incorporating cybersecurity risk evaluations into ED's IT investment management, project management, procurement, and resource management processes. ED will also enhance the Cybersecurity Framework (CSF) Risk Scorecard to mature and improve cybersecurity planning, awareness, and risk visualization around the IT portfolio. The Department will operationalize the Ongoing Security Authorization (OSA) Program to provide additional insight into information technology systems and services risks. A key focus of this objective is increasing phishing awareness and reporting rates while reducing susceptibility to phishing attacks.

Anticipated Outcome

The Department has a managed and measurable cybersecurity risk management program.

Objective 3.2: Enhance Cybersecurity Data Collection and Analysis Capabilities

In support of this objective, the Department will ensure that the increased use of data for program evaluation and policymaking is accompanied by improved privacy protections and transparency of data practices within ED and throughout the education community. The Department's efforts to improve privacy protections will focus on processes and procedures that drive day-to-day tasks while supporting advanced analytics and innovative techniques to track, collect, and analyze risk.

The Department will continue to grow data analytics capabilities around cybersecurity by developing a Cyber Data Lake and enhancing ED's Continuous Diagnostics and Mitigation (CDM) capabilities. ED will also establish data models and quality standards to ensure data quality, accessibility, and use informs cybersecurity risk decisions. Last, the Department will identify, develop, and provide training on policies, procedures, and practices that emphasize data-driven decision-making specific to cybersecurity.

Anticipated Outcome

The Department will achieve cybersecurity data dominance, which facilitates thorough and timely reporting and effective decision-making.

Objective 3.3: Implement Enterprise Controls to Reduce Risk

Under this objective, the Department will mature the Common Controls Catalog to ensure that risk management activities incorporate cybersecurity information and governance processes around shared risks are established. The Department will continue to improve standards around identity and access management, incident recovery, and contingency planning, including implementing an enterprise-wide Identity, Credentials, and Access Management (ICAM) solution and integrating ED systems with this solution. The Department will also mature existing security controls, including implementing and integrating Continuous Diagnostics and Mitigation (CDM) capabilities for Department systems. Last, ED will continue exploring and adapting modern types of controls, focusing on those that will result in cybersecurity risk reduction on an enterprise-wide scale, such as the adoption of Zero Trust controls and the maturation of Trusted Internet Connection (TIC) 3.0 capabilities.

Anticipated Outcome

The Department has mature capabilities in place to manage, monitor, and secure access to Department resources.

Objective 3.4: Establish a Threat Intelligence Management Program.

The Department will implement heightened threat management and counterintelligence capabilities using a phased approach. The approach will include creating insider threat technology policies, processes, and procedures to establish insider threats as a core objective in protecting IT applications, systems, and networks. As part of the approach, the Department will develop quantitative metrics to address the core competencies of the insider threat capability program to better track performance at the leadership level. ED will monitor emerging technical threats and vulnerabilities and modify measures as needed to enhance safeguards. The evolution of ED's threat management and counterintelligence capabilities will be accomplished in concert and collaboration with the Department's Federal Senior Intelligence Coordinator (FSIC) and law enforcement, as appropriate.

Anticipated Outcome

The Department has a mature threat intelligence management program designed to gather raw data about emerging or existing threat actors and threats from multiple sources and provides actionable and timely information to our cyber defender to bolster ED's threat posture

Objective 3.5: Mature the Department's Security Operations Centers

This objective outlines a unified and standardized approach to cybersecurity data collection and shared analytics through collaboration and Security Operations Center (SOC) maturation. This objective requires the collective effort of Department stakeholders to consolidate and streamline SOC processes where possible and improve ED's ability to engage in counterintelligence and enhanced threat management. To increase the overall maturity of ED's SOC, strengthen the protection of High Valued Assets (HVAs), and strengthen the security of ED's IT environment, ED will consolidate the SOC operations and develop continuous process improvements. This objective will streamline Tier I, II, and III incident response operations to optimize execution while reducing process duplication. The improved SOC environment will increase Tier III capabilities in advanced threat analysis, identity and access management, enhanced digital forensics, and security data collection and analysis through shared processes and team consolidation. The maturation of SOC functions will be guided by standard processes and procedures and increasing core competencies of the Department's analysts and forensics staff, including in the significant security areas of data loss prevention, intrusion prevention, incident triage, and incident management.

Anticipated Outcome

The Department has a managed and measurable security operations program.

Objective 3.6: Implement Zero Trust Architecture

The Department will adopt a Zero Trust Architecture (ZTA), following Executive Order 14028. A ZTA allows the Department to mitigate cybersecurity risks posed by modern cybersecurity threats in a complex multi-cloud environment more effectively and efficiently. The Department will follow the National Institute of Standards and Technology (NIST) Special Publication 800-207 ZTA guidelines to establish the ZTA strategy, architecture, and implementation roadmap.

A ZTA program will improve Department security infrastructure, increase visibility across the security environment, and enhance data protection. The Department's ZTA program will include a catalog of solutions intended to improve the security of IT systems and incorporate the standards and guidelines needed to foster adaptation of these solutions across a portfolio of IT services. The Department will adopt modern security best practices through this objective, including improving multi-factor authentication (MFA) and encryption for data at rest and in transit. The Department will continue delivering secure cloud services and centralizing and streamlining access to cybersecurity data to drive analytics for identifying and effectively managing cybersecurity risks. Last, the Department will invest in the technology and personnel needed to support these ZTA modernization goals.

Anticipated Outcome

The Department has a Zero Trust Program that establishes and executes the strategy, architecture, design, implementation roadmap, and catalog of Zero Trust services.

Strategic Goal 4

Improve the Department's IT Communications and Engagement

Goal Leader: OCIO Chief of Staff

Goal Overview

Department staff need to understand what IT resources and technology are available to meet their needs. Staff also need to understand how future technology changes will impact their work. Last, ED needs a comprehensive IT workforce development plan to ensure that the Department recruits, retains, and develops staff to meet future technology needs. Through this goal, the Department will develop an IT communications strategy that outlines how IT communications will be accessible, encourage staff engagement with IT initiatives, and are consistent and high-quality. Increasing the quality of IT communications will improve staff engagement with IT resources and requirements, compliance with applicable requirements, and return on IT investments.

IT operations' effectiveness also depends on having staff with the skills, competencies, and knowledge to use available IT resources. Therefore, the Department will proactively plan for the IT workforce needed by developing an agency IT workforce action plan. This plan will detail how the Department will ensure access to IT training resources, self-service IT resources through ED's intranet site, and regular, comprehensive communications about changes or updates impacting IT staff.

Investing in the Department's IT communication structure and IT workforce will improve the competencies and skills of the Department's workforce, both for IT and non-IT professionals. Increased IT competency will enhance staff's ability to engage in self-service and use the technology they need to be effective at their jobs. Last, improving staff's understanding of technology requirements, changes, and cybersecurity practices will also help minimize cybersecurity risk and improve agency compliance with important IT rules and regulations.

Anticipated Outcome

The Department regularly communicates about IT changes, training, and resources and has an IT workforce development plan that allows ED to proactively plan for a future workforce.

Objective 4.1: Enhance Enterprise IT Communications

The Department will develop and implement an IT communications strategy that prioritizes ED's users and customers. Regardless of the quality or clarity of IT communications, the effectiveness of those communications will be limited if they are not accessible. This objective includes a review of communications channels and delivery methods. The Department will use the analysis to identify where ED can consolidate, streamline, and improve the Department's overall effectiveness at keeping customers informed of technology changes and evaluate how and with what tools ED is delivering critical IT updates to support an increasingly mobile workforce.

Anticipated Outcome

The Department regularly, proactively, and consistently communicates with customers about enterprise IT changes, enhancements, and resources that may impact them personally by making sure that messaging is accessible, written in plain language, and is easy to find.

Objective 4.2: Strengthen the Department's IT Workforce

All ED staff, both IT professionals and non-IT professionals, should have a full range of IT-related skills and competencies to execute their duties effectively and efficiently. This objective focuses on developing a comprehensive IT workforce action plan that outlines the training, professional development

opportunities, and retention and recruitment strategies needed to ensure that ED has a highly competent technology-driven staff. IT workforce development strategies need to closely align with the Chief Human Capital Officer's (CHCO) overarching strategy for enterprise-wide workforce development and leverage applicable policies, guidance, processes, and tools. For ED's IT professionals, developing this plan means taking steps to map the competencies and standards that staff must meet to successfully execute their responsibilities, move to a different job, or advance in their field of expertise.

This objective will also include investing in and developing the workforce based on identifying emerging and mission-critical skills so that the Department is reskilling and redeploying employees from lower-value work activities to higher-value work activities. Last, the Department will use this plan to ensure a comprehensive and coordinated approach to IT related skill and competency development and deployment across the agency.

Anticipated Outcome

The Department has an IT workforce with the knowledge, skills, and capacity to successfully meet the agency's mission and is recruiting, retaining, and developing high-performing IT employees.

Appendix A: Relevant Laws, Regulations, and Resources

21st Century Integrated Digital Experience Act (21st Century IDEA:) requires all government-produced digital products, including websites and applications, to be consistent, modern, and mobile-friendly.

36 Code of Federal Regulations (CFR) B – Records Management: specifies policies for Federal agencies' records management programs relating to proper records creation and maintenance, adequate documentation, and records disposition.

Clinger-Cohen Act of 1996: eliminated the exclusive authority of the General Services Administration to acquire technology and allowed individual federal agencies to assume that role to improve the way the federal government acquires, uses, and disposes of information technology.

Evidence Act or H.R.4174 – Foundations for Evidence-Based Policymaking Act of 2018: requires agency data to be accessible and that agencies develop statistical evidence to support policymaking.

Executive Order 13556 – Controlled Unclassified Information (CUI): establishes a program for managing all unclassified information in the Executive branch that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies.

Executive Order 14028 – Improving the Nation's Cybersecurity: supports the nation's cybersecurity and protects the critical infrastructure and federal government networks underlying the nation's economy and way of life.

Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99): a federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Federal Information Security Modernization Act (FISMA) of 2014: codifies the Department of Homeland Security authority to administer the implementation of information security policies for non-national security federal Executive Branch systems, including providing technical assistance and deploying technologies to such systems, and reestablishes the oversight authority of the Director of the Office of Management and Budget.

Federal Information Technology Acquisition Reform Act (FITARA) of 2014: requires heads of agencies to ensure that their respective chief information officers have a significant role in information technology decisions, including annual and multi-year planning, programming, budgeting, execution, reporting, management, governance, and oversight functions.

Federal Records Act of 1950: establishes the framework for records management programs in federal agencies.

Government Performance and Results Act (GPRA) (1993, 2010): requires federal agencies to establish standards measuring their performance and effectiveness. Congress uses these standards to help guide budgetary decisions. GPRA Modernization Act of 2010 (Sec. 2) amends the Government Performance and Results Act of 1993 to require each executive agency to make its strategic plan available on its public website and to the Office of Management and Budget (OMB) on the first Monday in February of any year following that in which the term of the President commences and to notify the President and Congress.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 – Zero Trust Architecture: includes the core logical components that make up a zero trust architecture (ZTA) and gives general deployment models and use cases where zero trust could improve an enterprise's overall information technology security posture.

OMB/National Archives and Records Administration (NARA) Transition to Electronic Records Directive (M-21-19): a directive requiring that agencies eliminate paper, use electronic recordkeeping to the fullest extent possible, and create a robust records management framework that complies with statutes and regulations in an effort to reform records management policies and practices and to develop a 21st-century framework for the management of government records.

OMB, Revised Circular A-130: establishes general policy for information governance, acquisitions, records management, open data, workforce, security, and privacy while emphasizing the role of privacy and security in the federal information life cycle. Signals a shift from viewing security and privacy requirements as compliance exercises to understanding security and privacy as crucial elements of a comprehensive, strategic, and continuous risk-based program at federal agencies.

Privacy Act of 1974: establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

The Rehabilitation Act of 1973: sections 504 and 508 of the Rehabilitation Act of 1973 respectively require that agencies provide individuals with disabilities an equal opportunity to participate in their programs and benefit from their services, including the provision of information to employees and members of the public, and that agencies ensure that persons with disabilities (both employees and members of the public) have comparable access to and use of electronic information technology.

U.S. Department of Education Strategic Plan: describes the policy and operational priorities for the agency with details of the Department's strategic goal and objectives over a predetermined multi-year timeline.

U.S. Department of Education Data Strategic Plan: describes the Department's vision for accelerating progress toward becoming a data-driven organization and fully leveraging the power of data to advance the Department's mission of ensuring equal access and fostering educational excellence for the nation's learners.

Appendix B: List of Acronyms

CAP: Cross Agency Priority
CDM: Continuous Diagnostics and Mitigation
CDO: Chief Data Officer
CHCO: Chief Human Capital Officer
CIO: Chief Information Officer
CSF: Cybersecurity Framework
CUI: Controlled Unclassified Information
EA: Enterprise Architecture
ED: The Department of Education
EO: Executive Order
FSIC: Federal Senior Intelligence Coordinator
FY: Fiscal Year
HVAs: High Valued Assets
IRM: Information Resources Management
ICAM: Identity, Credentials, and Access Management
IT: Information Technology
ITIM: Information Technology Investment Management
MFA: Multi-Factor Authentication
NIST: National Institute of Standards and Technology
OCDO: Office of the Chief Data Officer
OCIO: Office of the Chief Information Officer
OSA: Ongoing Security Authorization
PMA: President's Management Agenda
POC: Principal Office Component
SOC: Security Operations Center
TBM: Technology Business Management
TIC: Trusted Internet Connection
ZTA: Zero Trust Architecture

Appendix C: Glossary

Accountability: the obligation to take responsibility for performance considering commitments and expected outcomes.

Common Controls Catalog: a shared, predetermined, and indexed set of management, operational, and technical safeguards or countermeasures employed within an organizational information system used to protect the confidentiality, integrity, and availability of the system and its information.

ConnectED: the Department of Education's enterprise intranet web portal, which contains sites and content viewable by all users within the ED network, presents information that is of Department-wide general interest, and is updated and maintained by group contributors, webmasters, and the ConnectED Management Team.

Continuous Diagnostics and Mitigation Capabilities: tool used to help ensure an ongoing state of security of federal information systems and applications, including conducting audit reviews and performing diagnostic testing to ensure operational procedures and warning systems are in place.

Continuous Improvement: a research-based, ongoing review process with a goal of increasing overall effectiveness and making positive, measurable impact on all stakeholders by focusing on and implementing three essential elements: learn and share, examine and plan, and act and evaluate.

Cyber Data Lake: a system or repository of data that is stored in its natural or raw format, usually object blobs or files, used for tasks such as reporting, visualization, advanced analytics, and machine learning.

Cybersecurity Framework (CSF) Risk Scorecard: the categorical breakdown, scoring, and representation of an organization's cybersecurity posture as benchmarked against the NIST Cybersecurity Framework.

ED.Gov: the Department of Education's public facing internet domain.

Enterprise Architecture: enterprise architecture is the process by which organizations standardize and organize IT infrastructure to align with business goals. These strategies support digital transformation, IT growth, and the modernization of IT as a department.

Federal Senior Intelligence Coordinator: the senior position within an individual executive branch department or agency that has been designated by the head of that organization to serve as the primary liaison between the respective department or agency and the intelligence community.

Goals: long-range performance targets that are consistent with the mission, usually requiring a commitment of resources towards the objectives critical to goal achievement. Goal achievement is required for an organization to realize its vision.

High Valued Assets: information or an information system that is so critical to an organization that the loss or corruption of this information or loss of access to the system would have serious impact to the organization's ability to perform its mission or conduct business.

Human Capital Capacity: the collective skills and knowledge of the workforce.

Identity, Credentials, and Access Management System: comprises the tools, policies, and systems that allow an organization to manage, monitor, and secure access to protected resources.

Information Technology Investment Management: a management process that provides for the identification, selection, control, and evaluation of business need-driven information technology investments across the investment lifecycle, using structured processes to minimize risks, maximize return on investments, and support decisions to maintain, migrate, improve, retire, or obtain IT investments.

Information Technology Modernization Roadmap: the strategy document for segment owners and decision makers to evaluate and make effective investment decisions about ED's IT portfolio and the transition from legacy systems.

Information Technology Workforce Development Plan: a blueprint for effective workforce planning that aligns IT workforce requirements to the needs of the agency, aiding in the development of a comprehensive picture of existing talent and capacity gaps.

Insider Threat: a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors, or business associates who might have insider information concerning the organization's security practices or computer systems.

Mission: the primary purpose of an organization.

Multi-Factor Authentication: sometimes referred to as two-factor authentication or 2FA, is a security enhancement that allows you to present two pieces of evidence – your credentials – when logging in to an account.

National Institute of Standards and Technology: founded in 1901, NIST is one of the nation's oldest physical science laboratories. Congress established the agency to remove a major challenge to U.S. industrial competitiveness at the time—a second-rate measurement infrastructure that lagged the capabilities of the United Kingdom, Germany, and other economic rivals. NIST measurements support the smallest of technologies to the largest and most complex of human-made creations—from nanoscale devices so tiny that tens of thousands can fit on the end of a single human hair up to earthquake-resistant skyscrapers and global communication networks.

National Institute of Standards and Technology Cybersecurity Framework: guidance on how both internal and external stakeholders of organizations can manage and reduce cybersecurity risk. It lists organization specific and customizable activities associated with managing cybersecurity risk and it is based on existing standards, guidelines, and practices.

Objectives: specific actions for achieving an organization's goals.

Ongoing Security Authorization Program: risk-based security authorization process that provides the Authorizing Official with near real-time insight into the security posture of an information system. Instead of periodically reviewing cumbersome lists of security controls, ongoing assessments are driven by dynamic risk-based events.

Principal Operating Component: a branch or subset of the Department with a discreet set of subject matter responsibilities that support the organizational mission.

Security Operations Center: a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

Strategic Initiative: a one-to-two-year project that must be complete to drive the success of an objective.

Trusted Internet Connection 3.0: the third iteration of an initiative to modernizing IT infrastructure that has recognized shifts in modern cybersecurity, redefined federal cybersecurity by consolidating network connections, and enhanced visibility and security measures throughout the federal network while assisting agencies in the adoption of new technology solutions.

Values: the values and philosophy of an organization that guide the behavior and decisions of its members. The values constitute the organization's value system.

Vision: an idealized view of where an organization will be or will look like in the future, assuming all goals are met. It is a statement intended to express both aspiration and inspiration.

Zero Trust Architecture: a network-based set of perimeters and network segmentation that assumes that there is no implicit trust granted to assets or user accounts based solely on their physical or network location or asset ownership to safeguard users, assets, workflows, and resources.

Zero Trust Controls: a set of parameters that treats all users as potential threats and prevents access to data and resources until the users can be properly authenticated and their access authorized.