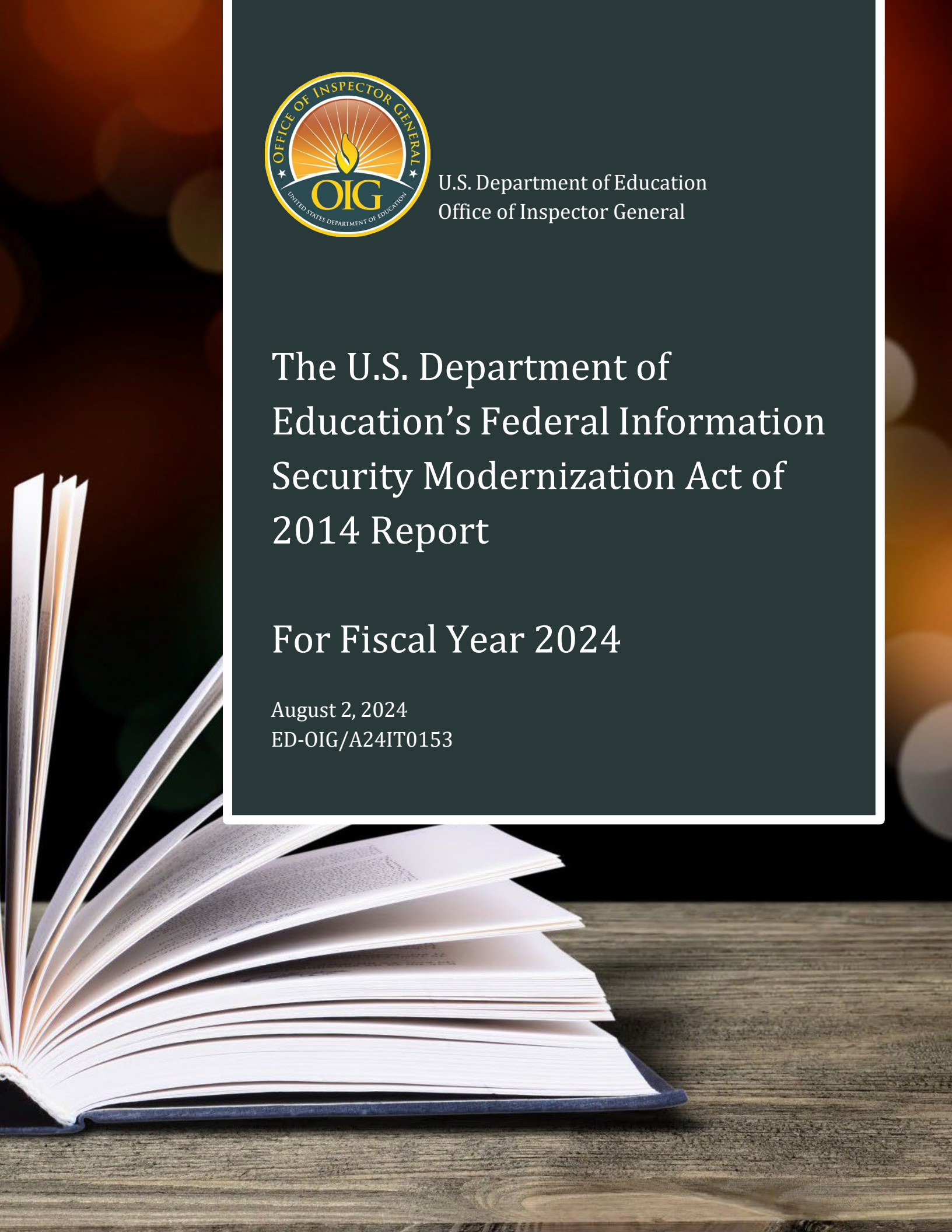

U.S. Department of Education
Office of Inspector General

The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report

For Fiscal Year 2024

August 2, 2024
ED-OIG/A24IT0153

August 2, 2024

TO: Brian Bordelon
Acting Chief Information Officer
Office of the Chief Information Officer

FROM: Antonio Murray /s/
Acting Assistant Inspector General
Technology Services
Office of Inspector General

SUBJECT: Final Audit Report
Federal Information Security Modernization Act of 2014 Audit of the U.S. Department of Education's Information Security Program and Practices for Fiscal Year 2024
Control Number ED-OIG/A24IT0153

Attached is the **final audit report** that determined whether the U.S. Department of Education's (Department) overall information technology security programs and practices are effective as they relate to Federal information security requirements. We contracted with the independent certified public accounting firm of Williams, Adley & Company – DC, LLC (Williams Adley) to conduct this audit. The audit assessed the information and information system security controls in place during the period of July 1, 2023, to June 30, 2024.

The contract required that the audit be performed in accordance with generally accepted government auditing standards (GAGAS). In connection with the contract, the Office of Inspector General (OIG) reviewed, provided feedback, and ultimately approved the audit plan. In addition, OIG monitored the performance of the audit, reviewed contractor audit documentation, attended critical meetings with the Department officials and reviewed the contractor's audit controls. As part of the oversight and monitoring, the OIG:

- ensured the audit complied with GAGAS and other OIG policies and procedures;
- ensured contract requirements regarding objectives, scope, and methodology were being met;
- held bi-weekly status meetings to discuss whether milestones were being met; and
- performed draft and final report reviews, conducted within Information Technology Audits, to provide assurance that the contractor's work can be relied upon.

An electronic copy has been provided to your Audit Liaison Officer. Williams Adley received and evaluated the Office of the Chief Information Officer (OCIO) management comments in response to the findings and recommendations in the report. OCIO agreed to provide corrective action plans for all recommendations by September 30, 2024.

Corrective actions proposed (resolution phase) and implemented (closure phase) by your office will be monitored and tracked through the Department's Audit Accountability and Resolution Tracking System. The corrective action plan should set forth the specific action items and targeted completion dates necessary to implement final corrective actions on the findings and recommendations contained in this final report.

In accordance with the Inspector General Act of 1978, as amended, the OIG is required to report to Congress twice a year on the audits that remain unresolved after 6 months from the date of issuance.

In accordance with the Freedom of Information Act (5 United States Code section 552), reports issued by the OIG are available to members of the press and general public to the extent information contained therein is not subject to exemptions in the Act.

Williams Adley is responsible for the enclosed auditor's report and the conclusions expressed therein. The OIG's review disclosed no instances where Williams Adley did not comply, in all material aspects, with GAGAS.

Should you or your office have any questions, please contact Joseph Maranto, Director, Information Technology Audits at 202-245-7044 or joseph.maranto@ed.gov.

Attachment

cc: Cindy Marten, Deputy Secretary, Office of the Deputy Secretary
James Kvaal, Under Secretary, Office of the Under Secretary
Denise Carter, Acting Chief Operating Officer, Federal Student Aid
Gary Stevens, Deputy Chief Information Officer, Office of the Chief Information Officer
Margaret Glick, Chief Information Officer, Federal Student Aid
Daniel Commons, Deputy Chief Information Officer, Federal Student Aid
Steven Hernandez, Chief Information Security Officer, Office of the Chief Information Officer
Davon Tyler, Chief Information Security Officer, Federal Student Aid
Bucky Methfessel, Senior Counsel for Information & Technology, Office of the General Counsel
Phil Rosenfelt, Deputy General Counsel, Office of General Counsel
L'Wanda Rosemond, Audit Accountability and Resolution Tracking System Administrator, Office of Inspector General

Audit Liaison Officers:
Samuel Rodeheaver, Office of the Chief Information Officer
Stefanie Clay, Federal Student Aid

Federal Information Security Modernization Act of 2014 Audit of the United States Department of Education's Information Security Program and Practices

Final Report for FY 2024

August 2, 2024

The statements within this report related to managerial practices need improvement, as well as other conclusions and recommendations, represent the opinions of the independent assessor, Williams Adley, under the oversight of the Office of Inspector General. Any appropriate corrective actions to address the conclusions within this report will be determined by the relevant U.S. Department of Education stakeholders. In accordance with Freedom of Information Act (Title 5, United States Code, Section 552), reports that the Office of Inspector General issues are available to members of the press and public to the extent information they contain is not subject to exemptions in the Act.

The contents of this draft report should not be shown or released for purposes other than official review and comment, except where required by law. This report must be safeguarded to prevent publication or improper disclosure of the information it contains.

WILLIAMS ADLEY

Mr. Brian Bordelon
Acting Chief Information Officer
Office of the Chief Information Officer
400 Maryland Avenue, SW
Washington, DC 20202

Dear Mr. Bordelon:

We are pleased to provide our report outlining the results of the performance audit conducted to determine the effectiveness of the U.S. Department of Education's (Department) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) for the fiscal year (FY) 2024 audit.

On December 4, 2023, the Office of Management and Budget (OMB) issued Memorandum M-24-04 ("Memorandum for the Heads of Executive Departments and Agencies: Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements") to provide instructions for meeting the FY 2024 FISMA reporting requirements.

To achieve this objective, we reviewed the FY 2023-2024 Inspector General FISMA reporting metrics and performance measures selected by OMB and conducted this performance audit in accordance with Generally Accepted Government Auditing Standards which requires that we obtain sufficient, appropriate evidence to provide a reasonable basis for our conditions and conclusions. We believe that the evidence obtained throughout the FY 2024 audit provides a reasonable basis for our conclusions and maturity ratings.

Based on the results of the audit procedures performed for the FY 2024 audit period, Williams Adley concluded that the Department has met the requirements to be operating at an effective level of security outlined within the FY 2024 FISMA reporting metrics for the subset of information system evaluated. The details supporting our overall conclusion is found in the attached report.

Additionally, we have included the Department's Management Response in Appendix D for your reference. Please note that Williams Adley has not audited the statements included in this the Management Response. We appreciate your cooperation and support during this audit. If you have any questions, please contact Tony Wang at Yong.Wang@ed.gov or (202) 631-1404.

/s/

August 2, 2024

Table of Contents

Results in Brief

The objective of the Fiscal Year (FY) 2024 Federal Information Security Modernization Act of 2014 (FISMA) audit was to determine whether the U.S. Department of Education (Department)'s overall information technology security program and practices are effective as they relate to Federal information security requirements.

To determine the effectiveness of the Department's information security program, Williams Adley utilized the FY 2023-2024 Inspector General (IG) FISMA reporting metrics[1], issued on February 10, 2023, which required that an independent assessor evaluate core and supplemental reporting metrics identified by the Office of Management and Budget (OMB).

To properly conclude on the effectiveness of the Department's information security program and practices, Williams Adley utilized a rotational strategy to select six in-scope systems[2] not evaluated in the prior year's audit.[3]

At the conclusion of the FY 2024 audit, Williams Adley determined that the Department's overall information technology (IT) security program and practices are effective as eight out of the nine FISMA domains met the requirements needed to operate at a Level 4 maturity rating or higher[4].

Additionally, Williams Adley identified a total of six conditions across the nine FISMA domains indicating potential areas of improvement for the Department. The identified conditions were evaluated from a risk-based standpoint and within the context of the overall information security program to determine their root cause and associated level of risk. For instances where an identified condition was related to an existing open recommendation, Williams Adley did not issue a new recommendation.

Table 1 and ***Table 2*** below outline the individual maturity ratings assigned to the core and supplemental metrics supporting the nine FISMA domains, and the calculated average maturity scores. The FY 2024 Audit Results section of this report outlines the individual scores for each metric question evaluated and any conditions identified.

[1] Final FY 2023 - 2024 IG FISMA Reporting Metrics v1.1 (cisa.gov)

[2] For the FY 2024 FISMA audit, Williams Adley selected Digital Customer Care, Education Security Tracking and Reporting System, Enterprise Technology Services – Integrated Services System, Unified Servicing and Data Solution – EDFinancial, Unified Servicing and Data Solution - Maximus Education/Aidvantage System, and the National Assessment Governing Board Website. Refer to Appendix A for details on scope selection criteria.

[3] A rotational strategy is used by Williams Adley to ensure that the implementation of the Department's information security program and practices are consistently implemented across its various information systems. This may result in significant changes to previously identified maturity levels in the event that defined activities are not operating as intended for the information systems selected for evaluation during the audit period.

[4] Within the context of FISMA, Level 4 (Managed and Measurable) is considered to be an effective level of maturity.

Function	Domain	Maturity Rating	Calculated Average
Identify	Risk Management	Managed and Measurable	4.40
Identify	Supply Chain Risk Management	Optimized	5.00
Protect	Configuration Management	Optimized	5.00
Protect	Identity and Access Management	Consistently Implemented	3.33
Protect	Data Protection and Privacy	Managed and Measurable	4.00
Protect	Security Training	Optimized	5.00
Detect	Information Security Continuous Monitoring	Optimized	5.00
Respond	Incident Response	Managed and Measurable	4.00
Recover	Contingency Planning	Optimized	5.00

Table 1 - FY 2024 Core Maturity Ratings

Function	Domain	Maturity Rating	Calculated Average
Identify	Risk Management	Managed and Measurable	4.00
Identify	Supply Chain Risk Management	Managed and Measurable	4.00
Protect	Configuration Management	Managed and Measurable	4.00
Protect	Identity and Access Management	Consistently Implemented	3.00
Protect	Data Protection and Privacy	Managed and Measurable	4.00
Protect	Security Training	Managed and Measurable	4.00
Detect	Information Security Continuous Monitoring	Managed and Measurable	4.00
Respond	Incident Response	Managed and Measurable	4.00
Recover	Contingency Planning	Managed and Measurable	4.00

Table 2 - FY 2024 Supplemental Maturity Ratings

Williams Adley also followed up on the status of outstanding recommendations to determine whether the Department has implemented their proposed corrective actions. Overall, Williams Adley determined that four prior year recommendations were closed. The status of the remaining recommendations is listed in Appendix B, Status of Prior-Year Recommendations, along with the proposed target action dates. As corrective actions are taken, the Office of Inspector General will examine the actions taken by Department management and close prior year recommendations, as applicable.

Lastly, Williams Adley prepared the responses to the core and supplemental metric questions identified within the CyberScope questionnaire, as shown in Appendix C. All Federal agencies are required to submit their IG FISMA metric determinations into the Department of Homeland Security's CyberScope application by July 31, 2024.

Background

United States Department of Education

The United States (U.S.) Department of Education (Department) is a governmental agency whose primary responsibility is to oversee and implement educational policies and programs. The mission of the Department is to promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access. The Department plays a crucial role in providing support and resources to educational institutions and systems. It allocates funding to schools and universities, assists in the development of educational infrastructure, and offers grants and scholarships to students. The Department also provides guidance and technical assistance to educational institutions, helping them enhance their programs, improve educational governance, and meet regulatory requirements.

In addition to these core functions, the Department often plays a role in shaping education policy at the national level. It collaborates with other government agencies, stakeholders, and educational experts to develop and implement education-related legislation and regulations. The Department conducts research and collects data on educational trends and outcomes to inform decision-making and policy development.

The Department is composed of multiple offices within the Office of the Secretary, Deputy Secretary, and Office of the Under Secretary. For the FY 2024 the Federal Information Security Modernization Act of 2014 (FISMA) audit, a representative subset of information systems within the Office of the Chief Information Officer (OCIO) and Federal Student Aid (FSA) were selected for evaluation[5].

The Department's OCIO advises and assists the Secretary and other senior officers in acquiring IT and managing information resources. OCIO helps these leaders to comply with the best practices in the industry and applicable federal laws and regulations, including the Clinger Cohen Act, the Government Paperwork Reduction Act and FISMA. In addition, the agency's Chief Information Officer (CIO) is charged with establishing a management framework that leads the agency toward more efficient and effective operations, including improved planning and control of IT investments.

The FSA office of the Department is the largest provider of student financial aid in the nation. FSA is responsible for managing the student financial assistance programs authorized under Title IV of the Higher Education Act of 1965. These programs provide grant, work-study, and loan funds to students attending college or career school. The FSA has its own CIO, whose primary responsibility is to promote the effective use of technology to achieve FSA's strategic objectives through sound technology planning and investments, integrated technology architectures and standards, effective systems development, and production support.

Federal Information Security Modernization Act of 2014

The Federal Information Security Management Act of 2002, part of the E-Government Act of 2002 (Public Law 107-347), recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act of 2002 required each agency to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support operations and assets, including those provided or managed by another agency or contractor. The E-Government Act of 2002 also assigned specific responsibilities to the Office of Management and Budget (OMB), agency heads, chief information officers, and Inspectors General. The Act established that OMB is responsible for creating and overseeing policies, standards, and guidelines for information security and has the authority to approve agencies' information

[5] Williams Adley selected one system managed by National Assessment Governing Board (NAGB), the NAGB Website. NAGB is an independent entity responsible for the oversight of its information systems and operates with the support of the Department.

security programs. Additionally, the Act established that the OMB is responsible for submitting an annual report to Congress, developing, and approving the cybersecurity portions of the President's Budget, and overseeing budgetary and fiscal issues related to the agencies' use of funds.

In 2014, the FISMA was enacted to update the Federal Information Security Management Act of 2002 by reestablishing the oversight authority of the Director of OMB with respect to agency information security policies and practices and setting forth authority for the Department of Homeland Security (DHS) Secretary to administer the implementation of such policies and practices for information systems. FISMA also provides several modifications that modernize Federal security practices to address evolving security concerns. These changes result in less overall reporting, stronger use of continuous monitoring in systems, increased focus on the agencies for compliance, and reporting that is more focused on the issues caused by security incidents. Furthermore, OMB regulations require Federal agencies to ensure that the appropriate officials are assigned security responsibilities and periodically review their information systems' security controls. Specifically, the agency's chief information officer is required to oversee the agency's information security program. Each agency must establish a risk-based information security program that ensures information security is practiced throughout the life cycle of each agency's systems.

The FISMA requires agencies to have an annual independent evaluation of their information security program and practices and to report the results to OMB and DHS via the CyberScope reporting tool. The FISMA states that the independent evaluation is to be performed by the agency Office of Inspector General (OIG) or an independent external auditor. Furthermore, the FISMA specifically mandates that each independent evaluation must include a test of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems and an assessment of the effectiveness of the information security policies, procedures, and practices of the agency.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Williams Adley utilized the FISMA metrics published by the OMB and the DHS, in consultation with the Council of the Inspectors General on Integrity and Efficiency (CIGIE), to evaluate the effectiveness of the Department's information security program and practices. The Inspector General FISMA reporting metrics are organized around the five security functions—Identify, Protect, Detect, Respond, and Recover— as outlined in National Institute of Standards and Technology (NIST)'s cybersecurity framework.

On December 4, 2023, the OMB issued Memorandum M-24-04 ("Memorandum for the Heads of Executive Departments and Agencies: Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements") to provide instructions for meeting the FY 2024 FISMA reporting requirements.

Section V of the Memorandum indicates that "OMB has selected a core group of metrics, representing a combination of Administration priorities and other highly valuable controls, that must be evaluated annually. The remainder of the standards and controls[6] are evaluated in metrics on a two-year cycle based on a calendar agreed to by CIGIE, the CISO Council, OMB, and CISA.

Maturity Model and Scoring Methodology

The OMB provided guidance to agency Inspector Generals or independent assessors for determining the maturity of their agencies' security programs through the publication of the FY 2023 – 2024 Inspector General FISMA Reporting Metrics. According to the reporting metrics, "the OMB believes that achieving a Level 4 (managed and measurable) or above represents an effective level of security"; see ***Table 3*** below for a definition of each maturity level.

[6] Also referred to as Supplemental Metrics.

Maturity Level	Description
Level 1 – Ad-Hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2 – Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3 – Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4 – Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5 – Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Table 3 – IG Evaluation Maturity Level Descriptions

Additionally, IGs and independent auditors are instructed to use "a calculated average approach, wherein the average of the metrics in a particular domain will be used by IGs to determine the effectiveness of individual function areas (identify, protect, detect, respond, and recover) and the overall program". As part of this approach, core metrics and supplemental metrics will be averaged independently to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness. This presents a shift from the "mode" based scoring methodology used in previous years where a domain and function's maturity rating were determined by a simple majority, the most frequent level across the questions served as the rating.

Furthermore, IGs and independent auditors are instructed that calculated averages will not be automatically rounded to a particular maturity level. Instead, the determination of maturity levels and the overall effectiveness of the agency's information security program should focus on the results of the core metrics and the calculated averages of the supplemental metrics as a data point to support their risk-based determination of overall program and function level effectiveness.

FY 2024 Audit Results

Williams Adley assessed the effectiveness of the Department of Education's information security program and practices on a maturity model where the foundational levels (Levels 1-2) ensure that policies and procedures are designed to support the requirements outlined within the Federal Information Security Modernization Act of 2014 (FISMA) and advanced levels (Levels 3-5) focus on the implementation and operating effectiveness of the defined policies and procedures. The following sections outline the results of our FY 2024 FISMA audit across all nine FISMA domains.

Identify

The Identify security function is comprised of the Risk Management and Supply Chain Risk Management metric domains. Based on our audit of the two program areas, Williams Adley determined that the Identify security function did meet the requirements of an effective information security program.

1) Risk Management

Risk management embodies the program and supporting processes to manage information security risks to organizational operations (including mission, functions, image, and reputation), organizational assets, staff, and other organizations.

Risk Management – Core Reporting Metrics

The OMB identified five reporting metrics as core for the development of a Risk Management program, as outlined in ***Table 4***:

Metric Question	Topic	FY 2024 Maturity Rating	FY 2023 Maturity Rating
1	Comprehensive and accurate inventory of agency information systems.	Level 4	Level 4
2	An up-to-date inventory of hardware assets.	Level 4	Level 4
3	An up-to-date inventory of software and associated licenses.	Level 4	Level 4
5	Information system security risks are adequately managed at all organization tiers.	Level 5	Level 4
10	Use technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities.	Level 5	Level 4

Table 4 – Ratings for Core Metric Questions within the Risk Management Domain

Based on the audit procedures performed and the scores outlined in ***Table 4*** above, Williams Adley determined that the Risk Management core metrics have a calculated average score of 4.40 and a maturity rating of Level 4 (Managed and Measurable)[7].

[7] The FY 2023-2024 IG FISMA Metrics state that "calculated averages will not be automatically rounded to a

Risk Management – Supplemental Reporting Metrics

The OMB identified two supplemental reporting metrics for evaluation in FY 2024, as outlined in ***Table 5***:

Metric Question	Topic	FY 2024 Maturity Rating	FY 2021 Maturity Rating[8]
4	Priority of information systems are categorized and communicated.	Level 4	Level 3
6	Information security architecture is used to provide a disciplined and structured methodology for managing risk and supply chain's risk.	Level 4	Level 3

Table 5 – Ratings for Supplemental Metric Questions within the Risk Management Domain

Based on the audit procedures performed and the scores outlined in ***Table 5*** above, Williams Adley determined that the Risk Management supplemental metrics have a calculated average score of 4.00 and a maturity rating of Level 4 (Managed and Measurable).

Metric Question Maturity Descriptions

Williams Adley concluded that the maturity of FISMA metric question 1 remains at a Level 4 (Managed and Measurable) maturity. Williams Adley found that the Department continues to implement its defined policies and procedures to maintain a comprehensive and accurate inventory of its information systems and system interconnections, and the Department's information systems are covered by its information security continuous monitoring (ISCM) processes[9].

Williams Adley concluded that the maturity of FISMA metric question 2 remains at a Level 4 (Managed and Measurable) maturity. Williams Adley found that the Department continues to implement its defined policies and procedures to maintain a comprehensive and accurate inventory of its information systems assets connected to the network and ensure they are covered the enterprise-wide hardware asset management capability and are subject to the monitoring processes defined within the Department's ISCM strategy. Additionally, Williams Adley did find missing required data elements in the hardware component inventories for following systems[10]:

- Enterprise Technology Services – Integrated Services Systems (ETS-ISS): Manufacturer Serial Number, and Date Device Added to System Boundary; and

particular maturity level." Furthermore, IGs or independent assessors are provided with the discretion to select the appropriate maturity rating based on the results of the audit procedures performed. Williams Adley believes that the current maturity of the activities associated with supplemental metrics do not significantly impact the agency's ability to manage risks within its organization.

[8] The FY 2024 supplemental FISMA reporting metrics were last evaluated during the FY 2021 reporting period.

[9] Within the context of the FY 2024 FISMA audit, the Department's ISCM program was deemed effective.

[10] Based on the audit procedures performed, Williams Adley did not identify any significant risk related to the missing data elements. Furthermore, this condition did not impact the Department's maturity rating as it was not deemed to be a pervasive issue across the hardware management process.

- Unified Servicing and Data Solution – Maximus Education/Aidvantage (USDS-MaxED/AidVntge: Active Directory (AD) Domain, Manufacturer Serial Number, Basic Input/Output System (BIOS) Universal Unique Identifier/Globally Unique Identifier (UUID/GUID) and Media Access Control (MAC) Address, and Date Device Added to System Boundary (Condition 1).

Williams Adley concluded that the maturity of FISMA metric question 3 remains at a Level 4 (Managed and Measurable) maturity. Williams Adley found that the Department has an organization-wide software asset management tool to identify and track software and its associated licenses within its environment. Additionally, the Department is utilizing a mobile device management tool to ensure that unauthorized software is not used on mobile devices. However, Williams Adley did find missing required data elements in the software component inventories for following systems[11]:

- ETS-ISS: Software Common Platform Enumeration (CPE) ID, Critical Software, Software/Database Vendor, License, License Expiration, Date Software Added to Inventory, Function, Environment, Hostname/Host ID, Date Software was First Detected on Device, Software Component Owner, Software Administrator, and First Tier Supplier
- Education Security Tracking and Reporting System (EDSTAR): Date Software Added to Inventory, Hostname/Host ID, Date Software was First Detected on Device, and First Tier Supplier
- USDS-MaxEd/AidVntge: License Expiration
- Unified Servicing and Data Solution – EDFinancial (USDS-EDF): Software CPE ID and Critical Software, Serial/License, Function, Environment, Software Host, Hostname/Host ID, Date Software was First Detected on Device, and First Tier Supplier (Condition 2).

Williams Adley concluded that the maturity of FISMA metric question 4 increased from a Level 3 to Level 4 (Managed and Measurable) maturity. Williams Adley found that the Department continues to implement its defined policies and procedures and ensures that the risk-based allocation of resources are completed based on system categorization, including for the protection of high value assets, as appropriate, through collaboration and data-driven prioritization.

Williams Adley concluded that FISMA metric question 5 increased from a Level 4 to Level 5 (Optimized) maturity. Williams Adley found that the Department has fully integrated the cybersecurity risk management at the organizational, mission/business process, and information system levels, as well as with its enterprise risk management program.

Williams Adley concluded that FISMA metric question 6 increased from a Level 3 to Level 4 (Managed and Measurable) maturity. Williams Adley found that the Department's information security architecture is integrated with its systems development lifecycle.

Williams Adley concluded that FISMA metric question 10 increased from Level 4 to Level 5 (Optimized) maturity, as the Department has integrated cybersecurity risk management into the enterprise risk management reporting processes and has institutionalized the use of advanced

[11] Based on the audit procedures performed, Williams Adley did not identify any significant risk related to the missing data elements. Furthermore, this condition did not impact the Department's maturity rating as it was not deemed to be a pervasive issue across the hardware management process.

technologies for analysis of trends and performance against benchmarks to continuously improve its cybersecurity risk management program.

The associated criteria for each identified condition is found in Appendix E.

Cause, Effect, and Recommendations

Williams Adley believes that the two conditions identified within the risk management domain are a result of the assigned Department and Federal Student Aid (FSA) personnel not completely entering the required attributes identified within the hardware and software inventory templates[12]. By not capturing all required data elements, the Department and FSA do not have a complete understanding of the hardware and software assets within their environment and may not be able to properly manage end of life hardware and software. To address the identified root causes, Williams Adley recommends that the Chief Information Officer require the Department and FSA to:

- Capture the missing hardware data elements for each identified system and assess whether other information systems may be missing similar or related data elements. (Recommendation 1.1).
- Further define the oversight controls that are in the current policy to ensure all Departmental systems consistently utilize the inventory template when completing/ updating the hardware inventory (Recommendation 1.2).
- Capture the missing software data elements for each identified system and assess whether other information systems may be missing similar or related data elements. (Recommendation 1.3).
- Further define the oversight controls that are in the current policy to ensure all Departmental systems consistently utilize the inventory template when completing/ updating the software inventory (Recommendation 1.4).

2) Supply Chain Risk Management

The Supply Chain Risk Management domain focuses on the maturity of agency strategies, policies and procedures, plans, and processes to ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain risk management requirements.

Supply Chain Risk Management – Core Reporting Metrics

The OMB identified one reporting metric as core for the development of a Supply Chain Risk Management program, as outlined in ***Table 6***:

[12] The inventory templates are designed to provide enterprise-wide guidance, including descriptions and examples, of which data elements are required or optional for hardware and software assets.

Metric Question	Topic	FY 2024 Maturity Rating	FY 2023 Maturity Rating
14	The agency ensures that products, system components, systems, and services of external providers are consistent with cybersecurity and supply chain requirements.	Level 5	Level 4

Table 6 – Ratings for Core Metric Questions within the Supply Chain Risk Management Domain

Based on the audit procedures performed and the scores outlined in ***Table 6*** above, Williams Adley determined that the Supply Chain Risk Management core metric has a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Supply Chain Risk Management – Supplemental Reporting Metrics

The OMB identified one supplemental reporting metric for evaluation in FY 2024, as outlined in ***Table 7***:

Metric Question	Topic	FY 2024 Maturity Rating	FY 2021 Maturity Rating
15	The agency ensures that counterfeit components are detected and prevented from entering the organization's system.	Level 4	Level 1

Table 7 – Ratings for Supplemental Metric Questions within the Supply Chain Risk Management Domain

Based on the audit procedures performed and the scores outlined in ***Table 7*** above, Williams Adley determined that the Supply Chain Risk Management supplemental metrics have a calculated average score of 4.00 and a maturity rating of Level 4 (Managed and Measurable).

Metric Question Maturity Descriptions

Williams Adley identified an increase in the maturity rating for FISMA metric question 14 from Level 4 to Level 5 (Optimized), as the Department continued to implement its processes to assess and review supply chain risks. Furthermore, the Department utilizes qualitative and quantitative performance metrics to monitor the information security and supply chain risk management performance of external providers. Lastly, the Department analyzes, in a near-real time basis, the impact of material changes to security and SCRM assurance requirements on its relationships with external providers and ensures that acquisition tools, methods, and processes are updated as soon as possible.

Williams Adley identified an increase in the maturity for FISMA metric question 15 from Level 1

to Level 4 (Managed and Measurable) maturity, as the Department implemented its processes to assess and review supply chain risks. Furthermore, the Department utilizes qualitative and quantitative performance metrics to monitor the effectiveness of its component authenticity policies and procedures and ensure that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.

Cause, Effect, and Recommendations

Williams Adley did not identify any conditions related to the Department's supply chain risk management program.

Protect

The Protect security function is comprised of Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training metric domains. Based on our audit of the four program areas, Williams Adley determined the Protect function is effective although the Identity and Access Management domain did not meet the requirements of an effective information security program.

3) Configuration Management

Configuration management includes tracking an organization's hardware, software, and other resources to support networks, systems, and network connections. This includes managing software versions and ensuring that updates installed on the organization's systems.

For the FY 2024 FISMA audit, Williams Adley contracted with Bulletproof to perform a vulnerability assessment of the in-scope systems. No significant issues were identified that impact the maturity determination of the Department's Configuration Management program and the results of the assessment were provided to Department Management within a separate report.

Configuration Management – Core Reporting Metrics

The OMB identified two reporting metrics as core for the development of a Configuration Management program, as outlined in ***Table 8***:

Metric Question	Topic	FY 2024 Maturity Rating	FY 2023 Maturity Rating
20	Use of configuration settings and common secure configurations.	Level 5	Level 4
21	Use of flaw remediation processes.	Level 5	Level 4

Table 8 – Ratings for Core Metric Questions within the Configuration Management Domain

Based on the audit procedures performed and the scores outlined in ***Table 8*** above, Williams Adley determined that the Configuration Management core metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Configuration Management – Supplemental Reporting Metrics

The OMB identified three supplemental reporting metrics for evaluation in FY 2024, as outlined in ***Table 9*:**

Metric Question	Topic	FY 2024 Maturity Rating	FY 2021 Maturity Rating
17	The roles and responsibilities of configuration management stakeholders.	Level 4	Level 4
18	Use of processes for identifying and managing configuration items during the appropriate phase within an organization's Software Development Life Cycle (SDLC).	Level 4	Level 4
23	Use of implemented configuration change control activities.	Level 4	Level 3

Table 9 – Ratings for Supplemental Metric Questions within the Configuration Management Domain

Based on the audit procedures performed and the scores outlined in ***Table 9*** above, Williams Adley determined that the Configuration Management supplemental metrics have a calculated average score of 4.00 and a maturity rating of Level 4 (Managed and Measurable).

Metric Question Maturity Descriptions

Williams Adley determined that FISMA metric question 17 remains at a Level 4 (Managed and Measurable) maturity, as the Department ensures that stakeholders are performing their defined roles and responsibilities. Moreover, the Department allocates resources in a risk-based manner to allow for stakeholders to effectively perform information system configuration management activities.

Williams Adley determined that FISMA metric question 18 remains at a Level 4 (Managed and Measurable) maturity, as the Department continues to execute its configuration management plan and supporting activities. Additionally, the Department monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its configuration management plan to make improvements as needed.

Williams Adley identified an increase in the maturity for FISMA metric question 20 from a Level 4 to Level 5 (Optimized) maturity, as the Department employs automation to maintain its common secure configurations.

Williams Adley identified an increase in the maturity for FISMA metric question 21 from a Level 4 to Level 5 (Optimized) maturity, as the Department centrally manages its flaw remediation processes and utilizes automation to ensure that patches are applied, as needed. Additionally, the

Department utilizes qualitative and quantitative performance measures on the effectiveness of flaw remediation processes to make improvements as needed.

Williams Adley identified an increase in the maturity for FISMA metric question 23 from a Level 3 to Level 4 (Managed and Measurable) maturity, as the Department uses qualitative and quantitative performance measures to monitor and evaluate the effectiveness of its change control activities.

Cause, Effect, and Recommendations

Williams Adley did not identify any conditions related to the Department's configuration management program.

4) Identity and Access Management

Identity and Access Management refers to identifying users, using credentials, and managing user access to network resources. It also includes managing the user's physical and logical access to Federal facilities and network. Remote access allows users to remotely connect to internal resources while working from a location outside their normal workspace. Remote access management is the ability to manage all connections and computers that remotely connect to an organization's network. To provide an additional layer of protection, remote connections should require users to connect using two-factor authentication.

Identity and Access Management – Core Reporting Metrics

The OMB identified three reporting metrics as core for the development of an Identity and Access Management program, as outlined in ***Table 10***:

Metric Question	Topic	FY 2024 Maturity Rating	FY 2023 Maturity Rating
30	Use of strong authentication mechanisms (Personal Identity Verification [PIV] or an Identity Assurance Level [IAL] 3/Authenticator Assurance Level [AAL] 3 credential) for non-privileged users.	Level 3	Level 3
31	Use of strong authentication mechanisms (PIV or an IAL 3/ AAL 3 credential for privileged users.	Level 4	Level 4
32	Privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties.	Level 3	Level 2

Table 10 – Ratings for Core Metric Questions within the Identity and Access Management Domain

Based on the audit procedures performed and the scores outlined in ***Table 10*** above, Williams Adley determined that the Identity and Access Management core metrics have a calculated average

score of 3.33 and a maturity rating of Level 3 (Consistently Implemented)[13].

Identity and Access Management – Supplemental Reporting Metrics

The OMB identified one supplemental reporting metrics for evaluation in FY 2024, as outlined in ***Table 11*:**

Metric Question	Topic	FY 2024 Maturity Rating	FY 2021 Maturity Rating
28	Processes for assigning position risk designations (PRDs) and performing appropriate personnel screening prior to granting access to its systems.	Level 3	Level 2

Table 11 – Ratings for Supplemental Metric Questions within the Identity and Access Management Domain

Based on the audit procedures performed and the scores outlined in ***Table 11*** above, Williams Adley determined that the Identity and Access Management supplemental metrics have a calculated average score of 3.00 and a maturity rating of Level 3 (Consistently Implemented)[14].

Metric Question Maturity Descriptions

Williams Adley identified an increase in the maturity for FISMA metric question 28 from Level 2 to Level 3 (Consistently Implemented) maturity, as the Department implemented its process to ensure all personnel are assigned risk designations, appropriately screened prior to being granted system access, and rescreened periodically. However, Williams Adley identified an issue with the execution of the Department's defined process as five (5) out of 22 PRDs sampled were signed after the investigation date. Furthermore, Williams Adley found that automation is not utilized to centrally document, track, and share risk designation and screening information (Condition 4).

Williams Adley determined that FISMA metric question 30 remains at the maturity level 3 (Consistently Implemented) maturity, as the Department does not implement strong authentication mechanisms for non-privileged users. Specifically, Williams Adley found the following conditions:

- The Department continued to deploy PIV-Alternative (ALT) configured GFEs to the Department users.
- 34 out of 445 sampled Department and FSA users were granted a short-term PIV-exemption for more than three (3) times.
- 860 Department users were granted long-term PIV-Exemption prior to the implementation of a process requiring submission for long-term PIV-Exemption extension request forms in October 2023.
- For 40 out of 40 sampled Department and FSA users, the respective Principal Offices (POs)

[13] Within the context of maturity model, Level 3 is considered to be ineffective.
[14] Within the context of maturity model, Level 3 is considered to be ineffective.

did not complete and submit the required long-term PIV-Exemption extension request forms (Condition 6).

Williams Adley determined that FISMA metric question 31 remains at a Level 4 (Managed and Measurable) maturity, as the Department continues to utilize strong authentication mechanisms for its privileged users, including those who can make changes to Domain Name System (DNS), to authenticate against organizational systems.

Williams Adley determined that FISMA metric question 32 remains at a Level 3 (Consistently Implemented) maturity, as the Department continues to execute its processes for provisioning, managing, and reviewing privileged accounts, employes restrictions on privileged user activities and ensures that their activities are logged and reviewed periodically. However, Williams Adley identified that the Department and the FSA did not consistently maintain the segregation of duties supporting the Privileged User Access (PUA) process. Specifically, for two (2) sampled privileged accounts, the creator/requestor and approver of the access request were the same person. Additionally, Williams Adley found that the Department is not meeting privileged identity and credential management logging requirements at maturity Event Logging (EL) 2, in accordance with Memorandum (M)-21-31 (Condition 5).

The associated criteria for each identified condition is found in Appendix E.

Cause, Effect, and Recommendations

Williams Adley believes that the conditions identified within the identity and access management domain are a result of the following identified root causes:

- The Department and FSA did not consistently oversee the decentralized process of reviewing and assigning the appropriate security background investigation prior to hiring new employees and contractors. Moreover, the Department and FSA did not ensure that PRDs are reviewed and signed prior to conducting the new hires security background investigation.
- The approver signed as the creator/requestor and approver for the two (2) access requests. In addition, the actual requestor made the request verbally and the approver granted their approval verbally, in violation of the policy.
- In response to the COVID-19 pandemic, the Department and FSA modified their process for onboarding personnel, including issuing PIV-ALT, to support continuing operations and the Department's mission. This change allowed users without access to credentialing service to be able to perform their roles and responsibilities. Since the end of the pandemic, the Department has continued to operate under the modified process and has not decided on how to move away from the over reliance of PIV alternates/exemptions.

Proper position designation is the foundation of an effective and consistent suitability and personnel security program. Without a process to ensure that new hires are provided with the appropriated security background investigation, the Department would not be able to effectively ensure there is no fraudulent activities or inappropriate behavior from the new hires that can pose a threat to the organization resources (People, information, systems). To address the identified root cause, Williams Adley recommends that the Chief Information Officer requires the Department

to:

- Implement a process to monitor that PRDs are reviewed and signed prior to the security investigation (Recommendation 2.1); and
- Implement an automation process to centrally document, track, and share risk designation and screening information (Recommendation 2.2).

Without proper documentation of access request approvals, the Department and FSA cannot ensure that users granted privileged access to the Department resources are appropriate based on their job responsibilities and accountability is maintained for the individuals granting the access. To address the identified root cause, Williams Adley recommends that the Department and FSA:

- Reinforce their process for documenting the authorization, review, and approval of PUAs (Recommendation 2.3); and
- Develop enhanced monitoring controls to ensure proper internal controls mechanisms and processes are strictly enforced (Recommendation 2.4).

Without a defined process to grant users PIV exemptions, monitor exemptions, and limit how often exemptions are granted, the Department and FSA increase the potential risk related to unauthorized access to its information systems. To address the identified root cause, Williams Adley recommends that the Chief Information Officer require Departmental Principal Offices re-evaluate the use of PIV alternates/exemptions across the organization, and modify onboarding procedures, as needed, to support a new strategic direction which aligns with HSPD-12 (Recommendation 2.5).

5) Data Protection and Privacy

Federal organizations have a fundamental responsibility to protect the privacy of individuals' Personal Identifiable Information (PII) that is collected, used, maintained, shared, and disposed of by programs and information systems. PII is any information about a person maintained by an agency that can be used to distinguish or trace a person's identity, such as name, Social Security number, date and place of birth, mother's maiden name, biometric records, and any other information that is linked or linkable to a person, such as medical, educational, financial, and employment information. Treatment of PII is distinct from other types of data because it needs to be not only protected, but also collected, maintained, and disseminated in accordance with Federal law.

Data Protection and Privacy – Core Reporting Metrics

The OMB identified two reporting metrics as core for the development of a Data Protection and Privacy program, as outlined in ***Table 12***:

Metric Question	Topic	FY 2024 Maturity Rating	FY 2023 Maturity Rating
36	Use of encryption of data rest, in transit, limitation of transference of data by removable media, and sanitization of digital media prior to disposal or reuse to protect its PII and other agency sensitive data.	Level 4	Level 4
37	Use of security controls to prevent data exfiltration and enhance network defenses.	Level 4	Level 4

Table 12 – Ratings for Core Metric Questions within the Data Protection and Privacy Domain

Based on the audit procedures performed and the scores outlined in ***Table 12*** above, Williams Adley determined that the Data Protection and Privacy core metrics have a calculated average score of 4.00 and a maturity rating of Level 4 (Managed and Measurable).

Data Protection and Privacy – Supplemental Reporting Metrics

The OMB identified two supplemental reporting metrics for evaluation in FY 2024, as outlined in ***Table 13***:

Metric Question	Topic	FY 2024 Maturity Rating	FY 2021 Maturity Rating
38	Development and implementation of a Data Breach Response Plan.	Level 4	Level 2
39	The privacy awareness training is provided to all individuals, including role-based privacy training.	Level 4	Level 3

Table 13 – Ratings for Supplemental Metric Questions within the Data Protection and Privacy Domain

Based on the audit procedures performed and the scores outlined in ***Table 11*** above, Williams Adley determined that the Data Privacy and Protection supplemental metrics have a calculated average score of 4.00 and a maturity rating of Level 4 (Managed and Measurable).

Metric Question Maturity Descriptions

Williams Adley determined that FISMA metric question 36 remains at a Level 4 (Managed and Measurable) maturity, as the Department continues to maintain its security controls to protect PII and ensures that the security controls for protecting PII and other agency sensitive data are subject to the monitoring processes defined within the Department's Information Security Continuous Monitoring (ISCM) strategy.

Williams Adley determined that FISMA metric question 37 remains at a Level 4 (Managed and Measurable) maturity, as the Department analyzes qualitative and quantitative measures to evaluate the performance of its data exfiltration and enhanced network defenses. Additionally, the Department conducted exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses.

Williams Adley identified an increase in the maturity for FISMA metric question 38 from a Level 2 to Level 4 (Managed and Measurable) maturity, as the Department consistently implemented its data breach response plan and utilized qualitative and quantitative measures on the performance measures of its plan to make improvements, as needed.

Williams Adley identified an increase in the maturity for FISMA metric question 39 from a Level 3 to Level 4 (Managed and Measurable) maturity, as the Department measured the effectiveness of its privacy awareness training program by obtaining feedback on the content of the training and conducting targeted phishing exercises for those with responsibility for PII. Additionally, the Department made updates to its training program based on feedback and a changing regulatory landscape.

Cause, Effect, and Recommendations

Williams Adley did not identify any conditions related to the Department's data protection and privacy management program.

6) Security Training

Security awareness training is a formal process for educating employees and contractors about IT security pertaining to the confidentiality, integrity, and availability of information. This includes ensuring that all people involved in using and managing IT understand their roles and responsibilities related to the organizational mission; understand the organization's IT security policy, procedures, and practices; and have adequate knowledge of the various management, operational, and technical controls required to protect the IT resources for which they are responsible.

Security Training – Core Reporting Metrics

The OMB identified one reporting metric as core for the development of Security Training program, as outlined in ***Table 14***:

Metric Question	Topic	FY 2024 Maturity Rating	FY 2023 Maturity Rating
42	Use of assessments of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training.	Level 5	Level 4

Table 14 – Ratings for Core Metric Questions within the Security Training Domain

Based on the audit procedures performed and the scores outlined in ***Table 14*** above, Williams Adley determined that the Security Training core metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Security Training – Supplemental Reporting Metrics

The OMB identified two supplemental reporting metrics for evaluation in FY 2024, as outlined in **Table 15**:

Metric Question	Topic	FY 2024 Maturity Rating	FY 2021 Maturity Rating
44	Security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems.	Level 4	Level 3
45	Use of specialized security training.	Level 4	Level 3

Table 15 – Ratings for Supplemental Metric Questions within the Security Training Domain

Based on the audit procedures performed and the scores outlined in ***Table 15*** above, Williams Adley determined that the Security Training supplemental metrics have a calculated average score of 4.00 and a maturity rating of Level 4 (Managed and Measurable).

Metric Question Maturity Descriptions

Williams Adley identified an increase in the maturity for FISMA metric question 42 from a Level 4 to Level 5 (Optimized) maturity, as the Department's personnel collectively possess a training level such that the Department can demonstrate that security incidents resulting from personnel actions or inactions are being reduced over time.

Williams Adley identified an increase in the maturity for FISMA metric question 44 from a Level 3 to Level 4 (Managed and Measurable) maturity, as the Department measured the effectiveness of its awareness program by conducting phishing exercises and follows up with additional awareness, training, and/or disciplinary action, as appropriate. Furthermore, the Department utilizes qualitative and quantitative performance measures to evaluate the effectiveness of its security awareness program and make improvements, as needed.

Williams Adley identified an increase in the maturity for FISMA metric question 45 from a Level 3 to Level 4 (Managed and Measurable) maturity, as the Department obtained feedback on its specialized security training content and processes and made updates to its program, as appropriate. In addition, the Department measured the effectiveness of its specialized security training program by conducting targeted phishing exercises and following up with additional training, and/or disciplinary action, as appropriate.

Cause, Effect, and Recommendations

Williams Adley did not identify any conditions related to the Department's security training program.

Detect

The Detect security function is comprised of the ISCM metric domain. Based on our audit of the program area, Williams Adley determined that the ISCM security domain does meet the requirements of an effective information security program.

7) Information Security Continuous Monitoring

Continuous monitoring of organizations and information systems determines the ongoing effectiveness of deployed security controls; changes in information systems and environments of operation; and compliance with legislation, directives, policies, and standards.

ISCM – Core Reporting Metrics

The OMB identified two reporting metrics as core for the development of a ISCM program, as outlined in ***Table 16***:

Metric Question	Topic	FY 2024 Maturity Rating	FY 2023 Maturity Rating
47	Use of ISCM policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier.	Level 5	Level 4
49	Performance of ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls.	Level 5	Level 4

Table 16 – Ratings for Core Metric Questions within the ISCM Domain

Based on the audit procedures performed and the scores outlined in ***Table 16*** above, Williams Adley determined that the ISCM core metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

ISCM – Supplemental Reporting Metrics

The OMB identified one supplemental reporting metric for evaluation in FY 2024, as outlined in ***Table 17***:

Metric Question	Topic	FY 2024 Maturity Rating	FY 2021 Maturity Rating
50	Process for collecting and analyzing ISCM performance measures and reporting findings.	Level 4	Level 3

Table 17 – Ratings for Supplemental Metric Questions within the ISCM Domain

Based on the audit procedures performed and the scores outlined in ***Table 17*** above, Williams Adley determined that the ISCM supplemental metrics have a calculated average score of 4.00 and a maturity rating of Level 4 (Managed and Measurable).

Metric Question Maturity Descriptions

Williams Adley identified an increase in the maturity for FISMA metric questions 47 and 49 from a Level 4 to Level 5 (Optimized) maturity, as the Department's ISCM policies and strategy are fully integrated with its enterprise and supply chain risk management, configuration management, incident response, and business continuity programs. In addition, the Department demonstrated that it is using its ISCM policies and strategy to reduce the cost and increase the efficiency of security and privacy programs.

Williams Adley identified an increase in the maturity for FISMA metric question 50 from a Level 3 to Level 4 (Managed and Measurable) maturity, as the Department captures qualitative and quantitative performance measures on the performance of its ISCM program and utilizes the performance measures are utilized to deliver persistent situational awareness across the organization.

Cause, Effect, and Recommendations

Williams Adley did not identify any conditions related to the Department's ISCM program.

Respond

The Respond security function is comprised of the Incident Response metric domain. Based on our audit of the program area, Williams Adley determined that the Incident Response security domain does meet the requirements of an effective information security program.

8) Incident Response

An organization's incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited to prevent future occurrences, and restoring IT services. The goal of the incident response program is to provide surveillance, situational monitoring, and cyber defense services; rapidly detect and identify malicious activity and promptly subvert that activity; and collect data and maintain metrics that demonstrate the impact of the Department's cyber defense approach, its cyber state, and cyber security posture.

Incident Response – Core Reporting Metrics

The OMB identified two reporting metrics as core for the development of an Incident Response program, as outlined in ***Table 18***:

Metric Question	Topic	FY 2024 Maturity Rating	FY 2023 Maturity Rating
54	Processes for incident detection and analysis.	Level 3	Level 3
55	Processes for incident handling.	Level 5	Level 4

Table 18 – Ratings for Core Metric Questions within the Incident Response Domain

Based on the audit procedures performed and the scores outlined in ***Table 18*** above, Williams Adley determined that the Incident Response core metrics have a calculated average score of 4.00 and a maturity rating of Level 4 (Managed and Measurable).

Incident Response – Supplemental Reporting Metrics

The OMB identified three supplemental reporting metrics for evaluation in FY 2024, as outlined in ***Table 19***:

Metric Question	Topic	FY 2024 Maturity Rating	FY 2021 Maturity Rating
52	Coordinated approach to responding to incidents.	Level 4	Level 4
53	Roles, responsibilities, levels of authority, and level of dependencies of incident response team.	Level 4	Level 3
56	Incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders.	Level 4	Level 2

Table 19 – Ratings for Supplemental Metric Questions within the Incident Response Domain

Based on the audit procedures performed and the scores outlined in ***Table 19*** above, Williams Adley determined that the Incident Response supplemental metrics have a calculated average score of 4.00 and a maturity rating of Level 4 (Managed and Measurable).

Metric Question Maturity Descriptions

Williams Adley determined that FISMA metric question 52 remains at a Level 4 (Managed and Measurable) maturity, as the Department monitors and analyzes the qualitative and quantitative performance measures that were defined in its incident response plan to monitor and maintain the effectiveness of its overall incident response capability.

Williams Adley determined that FISMA metric question 53 remains at a Level 4 (Managed and Measurable) maturity, as the Department ensures that the resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement incident response activities. Furthermore, the Department ensures that the stakeholders are held accountable for carrying out their roles and responsibilities effectively.

Williams Adley determined that FISMA metric question 54 remains at a Level 3 (Consistently Implemented) maturity[15], as the Department is working towards implementing the logging requirements outlined within OMB Memorandum M-21-31[16]. Additionally, Williams Adley concluded that the Department continues to consistently implement its processes to detect and analyze incidents.

Williams Adley identified an increase in the maturity for FISMA metric question 55 from a Level 4 to Level 5 (Optimized) maturity as the Department utilizes dynamic reconfiguration to stop attacks, misdirect attackers, and to isolate components of systems.

Williams Adley identified an increase in the maturity for FISMA metric question 56 from Level 2 to Level 4 (Managed and Measurable) maturity, as the Department utilizes metrics to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.

Cause, Effect, and Recommendations

Williams Adley did not identify any conditions related to the Department's incident response program.

Recover

The Recover security function is comprised of the Contingency Planning metric domain. Based on our audit of the program area, Williams Adley determined that the Contingency Planning security domain does meet the requirements of an effective information security program.

9) Contingency Planning

Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocating information systems and operations to an alternate site, recovering information system functions using alternate equipment, or performing information system functions using manual methods.

Contingency Planning – Core Reporting Metrics

The OMB identified two (2) reporting metrics as core for the development of an Incident Response program, as outlined in ***Table 20***:

[15] Within the context of maturity model, Level 3 is considered to be ineffective.

[16] A recommendation will not be issued as the Department has an existing corrective action plan to address the missing logging requirements.

Metric Question	Topic	FY 2024 Maturity Rating	FY 2023 Maturity Rating
61	Business impact analyses (BIA) are used to guide contingency planning efforts.	Level 5	Level 4
63	Performance of information system contingency plan (ISCP) tests/exercises.	Level 5	Level 4

Table 20 – Ratings for Core Metric Questions within the Contingency Planning Domain

Based on the audit procedures performed and the scores outlined in ***Table 20*** above, Williams Adley determined that the Contingency Planning core metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Contingency Planning – Supplemental Reporting Metrics

The OMB identified two supplemental reporting metrics for evaluation in FY 2024, as outlined in ***Table 21***:

Metric Question	Topic	FY 2024 Maturity Rating	FY 2021 Maturity Rating
62	Information system contingency plans are developed, maintained, and integrated with other continuity plans.	Level 4	Level 3
64	Information system backup and storage, including use of alternate storage and processing sites.	Level 4	Level 2

Table 21 – Ratings for Supplemental Metric Questions within the Contingency Planning Domain

Based on the audit procedures performed and the scores outlined in ***Table 21*** above, Williams Adley determined that the Contingency Planning supplemental metrics have a calculated average score of 4.00 and a maturity rating of Level 4 (Managed and Measurable).

Metric Question Maturity Descriptions

Williams Adley identified an increase in the maturity for FISMA metric question 61 from a Level 4 to Level 5 (Optimized) maturity as the Department's integrates its BIA and asset management processes with its enterprise risk management program to improve risk identification, accurate exposure consideration, and effective risk response.

Williams Adley identified an increase in the maturity for FISMA metric question 62 from a Level 3 to Level 4 (Managed and Measurable) maturity as the Department's utilizes metrics on the effectiveness of its various contingency plans to deliver persistent situational awareness across the

Department. In addition, the Department coordinated the development of ISCP's with the contingency plans of external service providers.

Williams Adley identified an increase in the maturity for FISMA metric question 63 from a Level 2 to Level 4 (Managed and Measurable) maturity, as the Department performed a full recovery and reconstitution of its information systems to a known state during the audit period. In addition, the Department proactively employed defined mechanisms to disrupt or adversely affect the system or system component and tested the effectiveness of contingency planning processes.

Williams Adley identified an increase in the maturity for FISMA metric question 64 from a Level 2 to Level 4 (Managed and Measurable) maturity, as the Department ensures that its information system backup and storage processes are assessed as part of its continuous monitoring program. In addition, as part of its continuous monitoring processes, the Department demonstrated that its system backup and storage and alternate storage and processing sites are configured to facilitate recovery operations in accordance with recovery time and recover point objectives. However, Williams Adley identified one (1) condition related to the Department's backup and storage processes, but it did not impact the maturity level of the question. Specifically, Williams Adley found that the Memorandum of Understanding (MOU) between the Unified Servicing and Data Solution – Maximus Education Aidvantage (USDS-MaxED/AidVntge) and Department of Education Amazon Web Services – East/West (EDAWSEW), dated June 16, 2022, was not updated, and approved on an annual basis (Condition 3).

Cause, Effect, and Recommendations

Williams Adley believes that the condition identified within the contingency planning program is the result of the Department and the Federal Student Aid (FSA) transitioning from a one year to a two-year review cycle and not appropriately updating the USDS-MaxED/AidVntge and EDAWSEW MOU to reflect the new review cycle. Without ensuring that the updated review cycles are incorporated/updated/reflected in the MOUs, the Department and FSA would not be able to effectively ensure that both parties to the contract are aligned in their objectives and understand their roles and responsibilities. To address the identified root cause, Williams Adley recommends that the Chief Information Officer require the Department and FSA to review and approve the USDS-MaxED/AidVntge and EDAWSEW MOU. Furthermore, the Department and FSA should update existing procedures and ensure all MOUs reflect the appropriate two-year review cycle (Recommendation 3.1).

Other Matters

As a part of the planning procedures for the FY 2024 Federal Information Security Modernization Act of 2014 (FISMA) audit, Williams Adley selected the National Assessment Governing Board (NAGB) Website (NAGBWeb) as an in-scope system for the evaluation of the U.S. Department of Education (Department)'s information security program.

Subsequently, as a part of the fieldwork phase, Williams Adley identified that NAGBWeb was not authorized following the guidelines outlined within National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision (Rev.) 2,[17] *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. By not following the suggested guidelines, the system may not be appropriately designed to minimize the potential impact of a security event and may introduce additional risk to an organization.

Per discussion with Department Management, it was determined that NAGB is an independent entity responsible for the oversight of its own information systems and operates with the support of the Department. As a result, the Department does not play an oversight role over the design of the system and Williams Adley will not issue a recommendation for the issue identified. Instead, this issue was included in this Other Matters section for the awareness of those charged with governance.

[17] NIST 800-37, Rev. 2 provides guidelines for applying the Risk Management Framework (RMF) to information systems and organizations. The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring.

Appendix A. Objectives, Scope, and Methodology

Objectives

The objective of the Fiscal Year (FY) 2024 Federal Information Security Modernization Act of 2014 (FISMA) audit was to determine whether the Department of Education (Department)'s overall information technology security program and practices are effective as they relate to Federal information security requirements.

The fieldwork for the FY 2024 audit began in October 2023 and ended in July 2024. For the FY 2024 audit, the Inspector General (IG) FISMA reporting metrics required that the agency Office of Inspector General (OIG) or an independent assessor evaluate the 20 core and 15 supplemental reporting metrics identified by the Office of Management and Budget (OMB).

To accomplish the two objectives, Williams Adley obtained an understanding of the Department's information security program and processes across the nine FISMA domains within the five security functions: (1) Risk Management, (2) Supply Chain Risk Management, (3) Configuration Management, (4) Identity and Access Management, (5) Data Protection and Privacy, (6) Security Training, (7) Information Security Continuous Monitoring, (8) Incident Response, and (9) Contingency Planning. Specifically, by

- Interviewing and inspecting written responses from the Department and Federal Student Aid (FSA) officials and contractor personnel, with knowledge of system security and application management, operational, and technical controls.
- Reviewing applicable information security regulations, standards, and guidance.
- Reviewing policies, procedures, and practices that the Department implemented at the enterprise and system levels.
- Obtaining and inspecting cloud service provider security packages for applicable systems through the Federal Risk and Authorization Management Program (FedRAMP) portal; and
- Meeting with Department and FSA key stakeholders to discuss enterprise and system-level security controls.

Additionally, Williams Adley conducted testing, including but not limited to the following, to verify processes and procedures were in place during the audit period:

- Reviewed corrective action plans for the last four FISMA audits (FY 2020 through FY 2023).
- Tested the design and implementation of management, operational, and technical controls based on NIST standards and Department guidance.
- Performed system-level testing for the Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, and Contingency Planning metric domains; and
- Conducted vulnerability assessments for in-scope Department and FSA systems, where applicable.

Scope

The FY 2024 audit covered the period July 1, 2023, to June 30, 2024, and was performed at the Department Office of Inspector General (OIG)'s Headquarters, Williams Adley Headquarters, and

remotely via Microsoft Teams.

To select the representative subset of information systems for the FY 2024 audit, Williams Adley obtained and inspected a population of 167 Department's FISMA Reportable Operational information systems from the Department's system of record, Cyber Security Assessment and Management System (CSAM). Williams Adley utilized the following criterion factors to select a judgmental sample of Department information systems:

- Federal Information Processing Standards (FIPS) 199 Categorization: "Moderate".
- New Systems added to the inventory.
- High-Value Asset (HVA) Systems.
- Systems containing Personally Identifiable Information (PII).
- No OIG Systems.
- Combination of Principal Offices (e.g., Office of Chief Information Officer, Federal Student Aid).
- Combination of non-cloud and cloud-dependent systems, including cloud service providers.
- Cybersecurity Risk Scorecard Results.

Based on the criteria above, Williams Adley identified a population of 21 systems and judgmentally selected the following 6 out of 21 systems based on the criteria mentioned above to determine the design and effectiveness of the Department's information security program:

- ETS-Integrated Services System (ETS-ISS)
- Digital Customer Care (DCC)
- Education Security Tracking and Reporting System (EDSTAR)
- Unified Servicing and Data Solution-Maximus Education/Aidvantage (USDS-MaxED/AidVntge)
- Unified Servicing and Data Solution-EDFinancial (USDS-EDF)
- National Assessment Governing Board Website (NAGBWeb)

Sampling Methodology

Williams Adley used nonstatistical audit sampling techniques, where applicable and appropriate, and utilized the AICPA Audit Guide: Audit Sampling, First Edition. Chapter 3: Nonstatistical and Statistical Audit Sampling in Tests of Controls. This guidance has been conformed to Statement on Auditing Standards (SAS) Nos. 122-125 and assists in applying audit sampling in accordance with AU-C section 530, *Audit Sampling* (AICPA, *Professional Standards*).

AU-C section 530, *Audit Sampling* allows auditors to use nonstatistical sampling for tests of controls. In addition, for a nonstatistical sampling approach, audit guidance allows auditors to use professional judgment to relate the same factors used in statistical sampling in determining the appropriate sample sizes. For nonstatistical sampling, Williams Adley used a sample selection approach that approximates a random sampling approach, including the following:

- **Simple Random Sampling**. Every combination of sampling units has the same probability of being selected as every other combination of the same number of sampling units. The auditor may select a random sample by matching random numbers generated by a computer.

- **Haphazard Sampling**. A haphazard sample is a nonstatistical sample selection method that attempts to approximate a random selection by selecting sampling units without a conscious bias, that is, without any special reason for including or omitting items from the sample (it does not imply the sampling units are selected in a careless manner).

Williams Adley used sampling to perform specific audit procedures and determine the operating effectiveness of control activities in the areas of Identity and Access Management, Data Protection and Privacy, Configuration Management, Security Training, and Incident Response.

FISMA Domain	Control Activity Description	Population Size	Sample Size
Identity and Access Management	Position Designation for New Users	3534	22
Identity and Access Management	Access Removal for Separated Employees and Contractors	237	23
Identity and Access Management	Privileged User Authorization	6260	22
Identity and Access Management	Personal Identity Verification (PIV) Exemption	1926	40
Configuration Management	Center for Internet Security (CIS) Deviations	11	2
Configuration Management	Configuration Change Requests	533	40
Data Protection and Privacy	Equipment Sanitization for Separated Employees and Contractors	237	40
Data Protection and Privacy	Breach Response Testing	56	5
Security Training	Required Security Training for New Users	6616	40
Security Training	Role-Based Training	85	23
Incident Response	Incident Resolution	45	5

Table 21 – Sample Sizes for Operating Effectiveness Testing

Use of Computer-Processed Data

For the FY 2024 audit, Williams Adley reviewed the security controls and configuration settings for the in-scope systems and applications externally hosted in a cloud environment. Williams Adley used computer-processed data for the Configuration Management, Identity and Access Management, Security Training, Data Protection and Privacy, and Incident Response metric domains to support the conclusions summarized in this report.

This data was obtained from the Department through self-reporting, generated through a system where auditors did not have rights to access the system, or obtained directly by Williams Adley via access granted by the Department.

Williams Adley performed assessments of the computer-processed data to determine whether the data were reliable for the purpose of our audit. To determine the extent of testing required for the assessment of the data's reliability, Williams Adley assessed the importance of the data and corroborated it with other types of available evidence. In cases where additional corroboration was needed, follow-up meetings were conducted. The computer-processed data was verified to source data and tested for accuracy according to relevant system controls until enough information was available to make a reliability determination. Finally, Williams Adley had access to the Department's security information repositories, including CSAM and the FedRAMP, to perform independent verification of evidence provided by the Department. Williams Adley determined data provided by the Department was reliable for the purpose of our audit.

Compliance with Standards

Williams Adley conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix B. Status of Prior Year Recommendations

Williams Adley followed up on the status of prior year recommendations to determine whether the Department of Education (Department) took corrective actions to address the identified issue(s) and/or root cause(s).

For instances where the Department took corrective actions, Williams Adley reviewed and tested implementation of the corresponding corrective action plan (CAP). If no issues were identified related to the CAP and associated testing, the recommendation was closed. If a CAP is outstanding or issues were identified in the related testing, the prior year recommendation remains open.

Based on the audit procedures for the Fiscal Year (FY) 2024 Federal Information Security Modernization Act of 2014 audit, Williams Adley determined that:

- The one FY 2020 recommendation remains open.
- There were no open FY 2021 recommendations.
- The only open FY 2022 recommendation was closed.
- Three out of six open FY 2023 recommendations were closed.

Details related to the individual prior year recommendations are found in the table below.

#	Description	Status	Target Action Date
FY 2020 1.4	We recommend that the Chief Information Officer (CIO) require the Department to establish and automate procedures to ensure all Department-wide IT inventories are accurate, complete, and periodically tested for accuracy. Include steps to establish that all IT contracts are reviewed and verified for applicable privacy, security, and access provisions. (Incorporates a Repeat Recommendation)	Open	09/30/2024
FY 2022 2.4	We recommend that the CIO require the Office of Chief Information Officer (OCIO) to establish and enforce a policy to maintain and track all privileged accounts in an authorized Privileged Access Management System(s).	Closed	10/31/2023
FY 2023 1.1	We recommend that the CIO require OCIO to implement additional measures for patches to be prioritized and applied within established timeframes.	Closed	02/14/2024
FY 2023 3.1	We recommend that the CIO require the Department to develop and implement an effective quality control review process for its policies and procedures.	Closed	12/12/2023
FY 2023 4.1	We recommend that the CIO require the Department and Federal Student Aid to take immediate corrective actions to remove users from the personal identity verification (PIV) exempt list.	Closed	12/12/2023

FY 2023 4.2	We recommend that the CIO require the Department to take immediate corrective actions for establishing quality control policies, procedures, and additional processes to ensure that user onboarding, elevated and non-elevated user access forms are properly completed, tracked, and maintained for records.	Open	8/29/2025
FY 2023 4.3	We recommend that the CIO require that the Department and Federal Student Aid (FSA) to take immediate corrective actions to ensure appropriate resources and funding are available and dedicated to complete implementation of the required EL1 and EL2 event logging maturities.	Open	12/31/2027
FY 2023 1.1.3	We recommend that the CIO require the Department to implement Cyber Security Assessment and Management System (CSAM) motives for security control assessment testing.	Open	7/31/2024

Appendix C. Responses to 2024 CyberScope Questionnaire

FISMA Question	Overall
.01	*Please provide an overall IG self-assessment rating (Effective/Not Effective).*
	Effective
.02	*Please provide an overall assessment of the agency's information security program. The narrative should include a description of the assessment scope, a summary on why the information security program was deemed effective/ineffective and any recommendations on next steps. Please note that OMB will include this information in the publicly available Annual FISMA Report to Congress to provide additional context for the Inspector General's effectiveness rating of the agency's information security program. OMB may modify the response to conform with the grammatical and narrative structure of the Annual Report.*
	The primary objective of the fiscal year (FY) 2024 FISMA audit was to determine whether the Department's overall information technology (IT) security programs and practices are effective as they relate to Federal information security requirements. The secondary objective of the FY 2024 FISMA audit was to determine the corrective actions taken by the Department to address previously identified and issued recommendations. To determine the effectiveness of the Department's information security program, Williams Adley utilized the following criterion factors to select a judgmental sample of Department information systems: • Federal Information Processing Standards (FIPS) 199 Categorization: "Moderate". • New Systems added to the inventory. • High-Value Asset (HVA) Systems. • Systems containing Personally Identifiable Information (PII). • No Office of Inspector General (OIG) Systems. • Combination of Principal Offices (e.g., Office of Chief Information Officer [OCIO], Federal Student Aid [FSA]); and • Combination of non-cloud and cloud-dependent systems, including cloud service providers. Williams Adley identified a population of 21 systems and judgmentally selected six to determine the design and effectiveness of the Department's information security program. At the conclusion of the FY 2024 audit, Williams Adley determined that eight out of nine FISMA domains (Risk Management, Supply Chain Risk Management, Configuration Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, and

	Contingency Planning) were effective, and the Department's overall IT security programs and practices were effective supporting the six in-scope systems.

FISMA Question	Risk Management
1	*To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third-party systems), and system interconnections?*
	Managed and Measurable Williams Adley determined that the Department has ensured that the information systems included in its inventory are subject to the monitoring processes defined within the Department's Information Security Continuous Monitoring (ISCM) strategy. In addition, the Department is working towards reflecting new system changes in near real time in the inventory to maintain a comprehensive and accurate inventory of the Department's information systems. However, the new system changes were comprehensively reflected in near real time in the Department's inventory for Fiscal Year (FY) 2024.
2	*To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE and Bring Your Own Device (BYOD) mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting?*
	Managed and Measurable Williams Adley determined that the Department has ensured that the hardware assets connected to the network are covered by the Department-wide hardware asset management capability and are subject to the monitoring processes defined within the Department's ISCM strategy. Furthermore, for mobile devices, the Department enforced the capability to deny access to the Department enterprise services when security and operating system updates have not been applied within a given period based on agency policy. In addition, the Department utilizes elements/taxonomy (e.g., Serial Number, Date Device Added to System Boundary, Active Directory Domain, Manufacturer Serial Number, Basics Input/Output, etc.) to track when the hardware is added to the environment, when it expires, etc. However, the Department did not consistently capture standard data elements/taxonomy for managing hardware inventory for two of its information systems. Specifically, Williams Adley found that the following data elements were missing within the respective system's hardware inventory: • Enterprise Technology Services – Integrated Services Systems (ETS-ISS): Manufacturer Serial Number, and Date Device Added to System Boundary; and • Unified Servicing and Data Solution – Maximus Education/Aidvantage (USDS-EDF): Active Directory (AD) Domain, Manufacturer Serial

	Number, Basic Input/Output System (BIOS) Universal Unique Identifier/Globally Unique Identifier (UUID/GUID) and Media Access Control (MAC) Address, and Date Device Added to System Boundary.
3	*To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?*
	Managed and Measurable Williams Adley determined that the Department has ensured that the software assets, including Executive Order (EO)-critical software and mobile applications as appropriate, on the network (and their associated licenses), are covered by the Department-wide software asset management (or Mobile Device Management) capability and are subject to the monitoring processes defined within the Department's ISCM strategy. Furthermore, the Department enforced the capability to prevent the execution of unauthorized software. However, the Department did not consistently capture standard data elements/taxonomy for managing software inventory for its systems. Specifically, Williams Adley found that the following data elements were missing within the respective system's hardware inventory: • Enterprise Technology Services – Integrated Services Systems (ETS-ISS): Software Common Platform Enumeration (CPE) ID, Critical Software, Software/Database Vendor, License, License Expiration, Date Software Added to Inventory, Function, Environment, Hostname/Host ID, Date Software was First Detected on Device, Software Component Owner, Software Administrator, and First Tier Supplier • Education Security Tracking and Reporting System (EDSTAR): Date Software Added to Inventory, Hostname/Host ID, Date Software was First Detected on Device, and First Tier Supplier • Unified Servicing and Data Solution – Maximus Education/Aidvantage (USDS-MaxEd/AidVntge): License Expiration • Unified Servicing and Data Solution – EDFinancial (USDS-EDF): Software CPE ID and Critical Software, Serial/License, Function, Environment, Software Host, Hostname/Host ID, Date Software was First Detected on Device, and First Tier Supplier
4	*To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets?*
	Managed and Measurable
5	*To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels?*
	Optimized
6	*To what extent does the organization use an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain?*

	Managed and Measurable
10	*To what extent does the organization use technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?*
	Optimized
11.1	*Please provide the assessed maturity level for the agency's Identify - Risk Management program.*
	Managed and Measurable
11.2	*Provide any additional information on the effectiveness (positive or negative) of the organizations risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?*
	Taking into consideration the maturity levels assigned to the Core and Supplemental metrics, Williams Adley concludes that the Department's risk management program is **effective**.

FISMA Question	Supply Chain Risk Management
14	*To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements?*
	Optimized
15	*To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization's systems?*
	Managed and Measurable
16	*Please provide the assessed maturity level for the agency's Identify - Supply Chain Risk Management program.*
	Optimized
16.1	*Please provide the assessed maturity level for the agency's Identify Function.*
	Managed and Measurable
16.2	*Provide any additional information on the effectiveness (positive or negative) of the organizations supply chain risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the supply chain risk management program effective?*
	Taking into consideration the maturity levels assigned to the Core and Supplemental metrics, Williams Adley concludes that the Department's supply chain risk management program is **effective**.

FISMA Question	Configuration Management
17	*To what extent have the roles and responsibilities of configuration management stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?*

	Managed and Measurable
18	*To what extent does the organization use an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems?*
	Managed and Measurable
20	*To what extent does the organization use configuration settings/common secure configurations for its information systems?*
	Optimized
21	*To what extent does the organization use flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management, to manage software vulnerabilities on all network addressable IP-assets?*
	Optimized
23	*To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the Change Control Board (CCB), as appropriate?*
	Managed and Measurable
25.1	*Please provide the assessed maturity level for the agency's Protect - Configuration Management program.*
	Optimized
25.2	*Provide any additional information on the effectiveness (positive or negative) of the organizations configuration management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?*
	Taking into consideration the maturity levels assigned to the Core and Supplemental metrics, Williams Adley concludes that the Department's configuration management program is **effective**.

FISMA Question	Identity and Access Management
28	*To what extent has the organization developed and implemented processes for assigning position risk designations and performing appropriate personnel screening prior to granting access to its systems?*

	Consistently Implemented Williams Adley determined that the Department has defined its processes for ensuring that all personnel are assigned risk designations and appropriately screened prior to being granted access to its systems. Processes have been defined for assigning risk designations for all positions, establishing screening criteria for individuals filling those positions, authorizing access following screening completion, and rescreening individuals on a periodic basis. Additionally, the Department ensures that all personnel are assigned risk designations, appropriately screened prior to being granted system access, and rescreened periodically. However, the Department does not employ automation to centrally document, track, and share risk designations and screening information with necessary parties.
30	*To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO2, or web authentication) for non-privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?*
	Consistently Implemented Williams Adley determined that the Department has consistently implemented strong authentication mechanisms for non-privileged users of the organization's facilities and networks, including for remote access, in accordance with Federal targets. For instances where it would be impracticable to use the PIV card, the organization uses an alternative token (derived PIV credential) which can be implemented and deployed with mobile devices. Further, for public-facing systems that support multifactor authentication, users are provided the option of using phishing-resistant multifactor authentication. Although, non-privileged users use strong authentication mechanisms to authenticate to applicable organizational systems and facilities. The Department continued to deploy PIV-Alternative configured Government Furnished Equipment (GFEs) to the Department users. Furthermore, the Department did not prevent user from being granted on short-term PIV-Exemption for more than three times, granted long-term PIV-Exemption to users prior to the process requiring submission for long-term PIV-Exemption extension request form, and the Principal Offices (POs) did not complete and submit required long-term PIV-Exemption extension request form.
31	*To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and nonprivileged users) that access its systems are completed and maintained?*
	Managed and Measurable
32	*To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO2, or web authentication) for nonprivileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?*
	Consistently Implemented

	Williams Adley determined that the Department has implemented its processes for provisioning, managing, and reviewing privileged accounts are consistently implemented across the organization. The Department limits the functions that can be performed when using privileged accounts; limits the duration that privileged accounts can be logged in; and ensures that privileged user activities are logged and periodically reviewed. Additionally, the Department employs automated mechanisms (e.g., machine-based, or user-based enforcement) to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate. However, the Department is not meeting privileged identity and credential management logging requirements at maturity Event Logging (EL)2, in accordance with Memorandum (M)-21-31.
34.1	*Please provide the assessed maturity level for the agency's Protect - Identity and Access Management program.*
	Consistently Implemented
34.2	*Provide any additional information on the effectiveness (positive or negative) of the organization's identity and access management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?*
	Taking into consideration the maturity levels assigned to the Core and Supplemental metrics, Williams Adley concludes that the Department's identity and access management program is **not effective**.

FISMA Question	Data Protection and Privacy
36	*To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle?*
	Managed and Measurable
37	*To what extent has the organization implemented security controls (e.g., EDR) to prevent data exfiltration and enhance network defenses?*
	Managed and Measurable
38	*To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events?*
	Managed and Measurable
39	*To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training?*
	Managed and Measurable
40.1	*Please provide the assessed maturity level for the agency's Protect - Data Protection and Privacy program.*
	Managed and Measurable
40.2	*Provide any additional information on the effectiveness (positive or negative) of the organizations data protection and privacy program that was not noted in the*

	questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the data protection and privacy program effective?
	Taking into consideration the maturity levels assigned to the Core and Supplemental metrics, Williams Adley concludes that the Department's data protection and privacy program is **effective**.

FISMA Question	Security Training
42	*To what extent does the organization use an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover?*
	Optimized
44	*To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems?*
	Managed and Measurable
45	*To what extent does the organization ensure that specialized security training is provided to individuals with significant security responsibilities (as defined in the organization's security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301)?*
	Managed and Measurable
46.1	*Please provide the assessed maturity level for the agency's Protect - Security Training program.*
	Managed and Measurable
46.2	*Please provide the assessed maturity level for the agency's Protect Function.*
	Managed and Measurable
46.3	*Provide any additional information on the effectiveness (positive or negative) of the organizations security training program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the security training program effective?*
	Taking into consideration the maturity levels assigned to the Core and Supplemental metrics, Williams Adley concludes that the Department's security training program is **effective**.

FISMA Question	Information Security Continuous Monitoring
47	*To what extent does the organization use ISCM policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier?*
	Optimized
49	*How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system?*
	Optimized

50	*How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings?*
	Managed and Measurable
51.1	*Please provide the assessed maturity level for the agency's Detect - ISCM function.*
	Optimized
51.2	*Provide any additional information on the effectiveness (positive or negative) of the organizations ISCM program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?*
	Taking into consideration the maturity levels assigned to the Core and Supplemental metrics, Williams Adley concludes that the Department's ISCM program is **effective**.

FISMA Question	Incident Response
52	*To what extent does the organization use an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents?*
	Managed and Measurable
53	*To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization?*
	Managed and Measurable
54	*How mature are the organization's processes for incident detection and analysis?*
	Consistently Implemented Williams Adley determined that the Department is working towards implementing the logging requirements outlined within OMB Memorandum M-21-31 which prevents them from achieving a higher maturity rating. Additionally, Williams Adley concluded that the Department continues to consistently implement its processes to detect and analyze incidents.
55	*How mature are the organization's processes for incident handling?*
	Optimized
56	*To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner?*
	Managed and Measurable
59.1	*Please provide the assessed maturity level for the agency's Respond - Incident Response function.*
	Managed and Measurable
59.2	*Provide any additional information on the effectiveness (positive or negative) of the organizations incident response program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the incident response program effective?*

	Taking into consideration the maturity levels assigned to the Core and Supplemental metrics, Williams Adley concludes that the Department's incident response program is **effective**.

FISMA Question	Contingency Planning
61	*To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts?*
	Optimized
62	*To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans?*
	Managed and Measurable
63	*To what extent does the organization perform tests/exercises of its information system contingency planning processes?*
	Managed and Measurable
64	*To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate?*
	Optimized
66.1	*Please provide the assessed maturity level for the agency's Recover - Contingency Planning function.*
	Optimized
66.2	*Provide any additional information on the effectiveness (positive or negative) of the organizations contingency planning program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the contingency program effective?*
	Taking into consideration the maturity levels assigned to the Core and Supplemental metrics, Williams Adley concludes that the Department's contingency planning program is **effective**.

Appendix D. Department of Education Management Response

UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF CHIEF INFORMATION OFFICER

DATE: July 31, 2024

TO: Antonio Murray
Acting Assistant Inspector General
Information Technology Audits and Computer Crime Investigations
Office of Inspector General

FROM: Brian Bordelon /s/
Acting Chief Information Officer
Department of Education

SUBJECT: Response to Federal Information Security Modernization Act of 2014 Audit of the United States Department of Education's Information Security Program and Practices Draft Report for FY 2024 Control Number I23IT0111.

Thank you for the opportunity to review and comment on the *Federal Information Security Modernization Act of 2014 Audit of the United States Department of Education's Information Security Program and Practices Draft Report for FY 2024*, Control Number ED-OIG/I23IT0111. The U.S. Department of Education (Department or ED) recognizes that the objective of the annual Office of Inspector General (OIG) Federal Information Security Modernization Act (FISMA) audit is to evaluate and determine the effectiveness of the Department's information security program policies, procedures, and practices. The Department is committed, and has taken numerous steps, to strengthen the overall cybersecurity of its networks, systems, and data.

Risk Management
The Department's accomplishments in maturing its risk management capabilities, specifically the maturation of the Cybersecurity Framework (CSF) Risk Scorecard, have been recognized by other Federal Agencies, including OMB, as an optimized capability in managing and communicating cybersecurity risk. The Department of Commerce (DOC), Department of Justice (DOJ), Department of Transportation (DOT), The United States Agency for International Development (USAID) and Nuclear Regulatory Commission (NRC) have all requested

playbooks for the development and implementation of CSF-based risk scoring capabilities in their environments based upon our constructs.

Throughout Fiscal Year (FY) 2024, the Department has continued its maintenance, enhancement, and capability of its CSF Risk Scorecard (v3.0), released in FY23. The ED CSF Risk Scorecard provides continuous performance measurement and risk prioritization of key metrics for system stakeholders, Principal Office Component (POC) leadership, and Department executive leadership on a daily, monthly, and quarterly basis. In FY24, the Department increased its daily report refresh frequency to three times daily to support more near-real time risk communication across the organization. The ED CSF Risk Scorecard also includes a daily Data Discrepancy Report (DDR) component that performs continuous validation of the information maintained within the Department's Governance Risk Compliance Tool (GRCT) to identify and correct inaccuracies.

During FY24, the Department began development of a new version of the CSF Risk Scorecard to align with NIST CSF v2.0, released in February 2024. In addition, the Department developed and released a Cyber Threat Intelligence Dashboard, integrated into the CSF Risk Scorecard, which incorporates a threat model for visualizing system threat susceptibility based on known vulnerabilities. This new threat model integration will further advance the Department's risk management capability maturity while also ensuring its evaluation of risk reflects both known vulnerabilities and threat vectors. The Department also released an updated Prioritized Risk Register within the CSF Risk Scorecard that incorporates threat calculations in prioritizing risk remediation activities. This enhancement further empowers system owners to quickly address those weaknesses and take action to improve their system's overall security posture. The Department also released an enhanced Automated Access Management process for the CSF Risk Scorecard, in alignment with our Departmental Standards, facilitating user access more efficiently.

The Department developed and implemented an updated version of the FISMA Quarterly Performance Dashboard. This updated report provides extensive automation of quarterly FISMA CIO metrics capture, evaluation, and performance measurement. Additionally, this report forecasts the Department's FISMA performance and the effectiveness of associated risk management activities across the Department based on projected OMB Cyber Progress scores within the tool. This has allowed the Department leadership and security professionals to take a more proactive approach in FISMA compliance.

The ED Cybersecurity Policy Working Group performed their annual review of ED policy standards. The annual review included incorporating guidance and mandates from all FY 2024 Office of Management and Budget (OMB) memoranda, Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) binding operational directives (BOD) and emergency directives (ED), as well as ED specific control overlays and enhancements.

The Department operationalized its Ongoing Security Assessment & Authorization (OSA) Program in accordance with roles and responsibilities established within the Information Technology (IT) System Security Assessment and Authorization (CA) Standard. ED has enrolled

80 FISMA reportable systems, 36 Cloud Service Providers (CSP), and 5 non-FISMA reportable subsystems into the OSA program since its adoption and has executed four (4) quarterly motive assessments. The Department is also working with DOJ to leverage and enhance OSA capabilities within GRCT to streamline OSA assessment execution and program reporting. This ensures the security risks of these systems are reported on a reoccurring basis to Department management and information system stakeholders' activities are being monitored through independent security assessments. This program reporting includes establishment of a Quarterly Assessment Report within which all OSA-related activities are documented. The highlights of that report are briefed each quarter to the Authorizing Official. Also established is a new OSA CSP Independent Verification and Validation (IV&V) report that serves as an annual report of the current security posture of the CSPs leveraged within the Department to ensure they remain within the Department's risk tolerance levels. The Department has also been able to establish a pen testing capability with the development of pen testing standard operating procedures, proposed penetration testing schedule, as well as CISA AES HVA training for assessors.

Supply Chain Risk Management
The Supply Chain Risk Management (SCRM) program integrated SCRM assessments with the ED Enterprise Architecture Technology Insertion process, also known as the EA (TI) process, to successfully identify 15 CFR Part 7 concerns with Adoptium, Otter.AI, and Avocent. Each company being owned presenting a significant Foreign Ownership, Control, or Influence (FOCI) risk. SCRM has also been integrated into the CSF Risk Scorecard to strengthen the ability to measure and monitor supply chain risks.

SCRM also contributed to the Small Business Innovation Research (SBIR) through Open-Source Intelligence (OSINT) assessments that are designed to give the SBIR program additional insight into potential companies conducting business with ED. SCRM has also compounded Rapid Vendor Assessments (RVAs) as a method to continuously assess vendors that ED utilizes. SCRM is using new SCRM tools, Interos and Lineaje. Interos is a real-time vendor risk scoring tool that SCRM utilizes as a starting point for all SCRM assessment types. Interos has created the ability for the SCRM to track on banned vendor lists released by the government, as well as gives up-to-date articles regarding the vendors in all areas from financial to cybersecurity posture. Lineaje is a real-time Software Bill of Materials (SBOM) tracking tool that we utilize as a centralized repository for vulnerability tracking and associative networked SBOMs, or dependency tracking from original SBOM which then associates other SBOMs as part of the cyber supply chain.

SCRM has integrated into FSA OSA process and contributes assessment packages that are presented to the FSA CISO on a quarterly basis. The contribution is necessary to give a holistic view of cyber supply chain risks associated with those systems and the assessment type aligns with the already established ED OSA process.

SCRM has been a cornerstone in the implementation of the Secure Software Attestation process, working with OPM, NASA, US State Dept, Microsoft, Google, and others regarding OMB M-22-18 and M-23-16 requirements and procedures. SCRM utilizes the DHS CISA Repository for Software Attestations and Artifacts (RSAA) as a centralized repository, sharing with federal agencies and reducing the burden on vendors. SCRM has assisted with the release of the ED

CISO Memo: Secure Software Development Attestation Form (SSDAF) collection which aligns ED schedules to that of M-22-18 and M-23-16 to ensure all applicable critical software SSDAFs for FISMA reportable information systems have been recorded and accurately documented in the information system software inventory within GRCT. The SCRM Provenance has been updated to include automations, parsing, and the associated data of all assessment types are fed into other risk scores in a compounding capacity. Data analytics has been realized for the SCRM Team in reading the underlying data to allow for informed decision making and reporting for ED. These new capabilities address the compliances of ED against new and novel governance such as OMB M-22-18 and are used in conjunction with CISA Repository for Attestations and Artifacts (RSAA) for attestation tracking and reporting.

Configuration Management

The Department expanded on its success in being the first to implement a Secure Access Service Edge (SASE) solution through its Technology Modernization Fund (TMF) award by optimizing SASE and Next Generation Firewall (NGFW) configurations. This included updating security rules to incorporate user identity and application layer filtering. The Department integrated its SASE solution with the CISA Cloud Aggregation Warehouse (CLAW). The Department implemented Endpoint Detection & Response (EDR) on cloud hosted servers. The Department also expanded its Security Orchestration Automation & Response (SOAR) capability to include automating Security Operation Center (SOC) procedures through automation playbooks. This has significantly increased SOC efficiency in responding to incidents. The Department awarded a cloud provider contract and in Q4 FY24 will finalize the TIC 3.0 architecture to be built into each hosting baseline. In Q4 FY24, the Department is implementing Software Defined Wide Area Network (SD-WAN) and Cloud Access Security Broker (CASB) to continue increasing maturity in ZTA. These efforts have enabled the Department to progress in adopting TIC 3.0. The Department's Tier III Zero Trust Architecture (ZTA) Program Management Office (PMO) drafted ZTA and Trusted Internet Connection (TIC) 3.0 control mappings and overlays to NIST 800-53 rev5 and is currently working to update Department policy and integrate into the Authority to Operate (ATO) process.

Identity and Access Management

The Department maintained its contract with a professional service provider to modernize and enhance its Enterprise Identity Credential and Access Management (ICAM) solution, which began September 1, 2022 and aligns with the OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* requirements to meet specific cybersecurity standards and objectives by the end of FY 2024. The ICAM program continues to provide improved security features and functionality which enhance the security posture of the Department.

The Enterprise ICAM program has been working to integrate all ED information systems with modern, phishing resistant authentication services, and has instituted a single sign-on (SSO) capability through a centralized user portal for ED employees and contractors to access Department applications and services, with 250 applications and services integrated to date. As a result, the Department improved the MFA compliance of its system inventory from 55% deployment at end of FY 2023 Quarter 1 to greater than 92% deployment at end of FY 2024 Quarter 2, exceeding the 90% target established by OMB in FY 2023 Quarter 3. From a data

encryption perspective, as of FY 2024 Quarter 3, the Department has achieved 97% data at rest (DAR) implementation compliance and 95% data in transit (DIT) compliance.

The Department's implementation of Certificate-based Authentication with Microsoft Entra ID by the Enterprise ICAM program was recognized by GSA for several best practices which have been incorporated into the FICAM Architecture implementation guidance[18] for all federal agencies. This implementation enabled the Department to adopt phishing-resistant multifactor authentication (MFA) with an X.509 certificate against its Public Key Infrastructure (PKI) directly between the Entra ID service and "relying party" applications/services across the Department. This bypasses the need for Active Directory Federation Services (ADFS) and enabled the full decommissioning of ADFS, which was completed this year.

In accordance with OMB M-22-09, the enterprise ICAM program has deployed two centrally managed phishing-resistant multifactor authentication (MFA) methods to serve as PIV-Alternate (PIV) methods when PIV or Derived PIV authentication are not available. These methods, FIDO2 security keys and Windows Hello for Business (WHfB), a Microsoft implementation of a Web Authentication-based authenticator, replace the legacy PIV-ALT single-factor authentication method (username/password), which is disallowed by M-22-09.
The Enterprise ICAM program has successfully maintained its Inter-Agency Agreement with GSA for the use of Login.gov to provide identity verification and authentication services for public users accessing Department applications and services. This includes the capability for public users to utilize several options for phishing-resistant multifactor authentication (MFA) which enables the Department to meet and exceed requirements set forth by OMB M-22-09[19].
The Enterprise ICAM program has coordinated with stakeholders across the Department to design, develop, test, and train users on its new digital identity lifecycle governance and administration (IGA) automation workflows, which automates provisioning of user account creation/disablement, birthright access, changes in user attributes and role-based access controls for individuals changing job roles/user types or leaving the Department. Additionally, this capability ensures that position risk designation forms are signed and uploaded prior to investigation dates and automates processes to centrally document, track, and share risk designation and screening information. The IGA automation workflows are planned to be deployed by the end of FY 2024.

The Enterprise ICAM program has added a new capability for Privileged Identity Management (PIM) via Entra ID which provides additional security controls for privileged user functions, including just-in-time privileged access to Entra ID and Azure resources, time-bound access to resources, requiring justification to understand why users activate privileged roles, notifications when privileged roles are activated, and audit history for privileged user activities.
Enterprise ICAM continues to maintain and enhance the following capabilities: self-service password reset (SSPR) functionality; certificate-based authentication (CBA) to support native personal identity verification (PIV) in cloud service provider (CSP) SSO; and identity lifecycle management (ILM) capabilities to enable automated user account provisioning and deprovisioning. Enterprise ICAM has also integrated with the ED Cyber Data Lake (EDCDL) to develop a centralized identity dashboard to improve transparency into identity related metrics

[18] Certificate-Based Authentication on Microsoft Entra ID Guide (idmanagement.gov)
[19] M-22-09 Federal Zero Trust Strategy (whitehouse.gov)

that align with OMB Memorandum M-22-09 and OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, for user and privileged user logging requirements.

FSA has made a number of enhancements to Access & Identity Management System (AIMS) and Person Authentication Service (PAS), allowing over 99 million students to better interact with FSA services, protect their accounts, and reduce the opportunity for potential fraud associated with compromised identities. FSA improved the account creation process by addressing the false positives being returned for legitimate No-SSN customers, for these No-SSN customers the system automatically creates a manual ID Verification case. The FSA Team also implemented a new password requirement to comply with IRS and addended the options for users to select the use of a passphrase which greatly strengthened the factor used in multi-factor authentication that is deployed by FSA.

Data Protection and Privacy

The ED Privacy Program is managed from the Office of Planning, Evaluation and Policy Development (OPEPD) Student Privacy Policy Office (SPPO) in coordination with the Office of the Chief Information Officer (OCIO). The Department Secretary designated a Senior Agency Official for Privacy (SAOP) who is responsible and accountable for developing, implementing, and maintaining the ED Privacy Program. The Privacy Program creates privacy policies, evaluates and manages privacy risks, and ensures compliance with all applicable statutes, regulations, and policies regarding the Department's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of personally identifiable information (PII).

In January 2024, the Department's Privacy Program launched a comprehensive connectED website that supports the Privacy Program and makes the Program's information, templates, policies, and other resources easily available to all Department staff and contractors. The new website includes:

- **Privacy Program Homepage** provides helpful information about the Privacy Program and basic privacy requirements.
- **PIAs/PTAs Page** provides templates and resources for developing privacy threshold analyses (PTAs) and privacy impact assessments (PIAs) for Department programs and systems.
- **SORNs/CMAs** Page provides resources for Privacy Act compliance, including system of records notices (SORNs) and computer matching agreements (CMAs).
- **Breach Response Page** provides information on breach response policies and procedures.
- **Privacy Training Page** provides resources on privacy awareness and training, including tips and useful information to increase your privacy knowledge.
- **Disclosure Review Board Page** provides information on the Department's Disclosure Review Board and resources for managing redisclosure risk when releasing data.
- **Policies/Guidance Page** provides information on Department and government-wide privacy policies.

During the reporting period, the Privacy Program updated the Department's Privacy Continuous Monitoring Strategy. The updated document modifies existing practices and establishes new monitoring practices. The Strategy ensures that privacy controls selected for information systems are effectively monitored on an ongoing basis at a frequency that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.
The Privacy Program planned and implemented a substantive, ED-wide Data Privacy Week awareness campaign. Activities included: webinars, ED-wide emails, and the launch of the Privacy Program's connectED webpage.

The Department developed two new policies on AI for use within the Department: (1) the Robotics Process Automation (RPA) and (2) the Artificial Intelligence (AI) Compliance Implementation Plan. The Privacy Program reviewed the documents to implement privacy policies and ensure consistency with privacy requirements. The policies have been uploaded to the appropriate Sharepoint site for privacy artifacts.

Security Training
The Department has clear policy (i.e., ACSD-OCIO-004 Cybersecurity Policy and ACSD-OCIO-003 Phishing Exercise Behavioral Based Escalations), standards (i.e., Awareness and Training [AT] Standard) and supporting standard operating procedures (i.e., Cybersecurity Training Program Consolidated SOP and Simulated Phishing Exercise SOP). These training program governance and process documents were reviewed and updated as part of program continuous monitoring. Updates to the IT Cybersecurity Awareness and Training Program Tactical Plan documented actions taken in FY 2023 and identified actions required to achieve plan goals in FY 2024. The FY 2023 to FY 2024 goals include institutionalizing processes for continuous improvement, promoting awareness, and reinforcing desired behaviors. Other goals include addressing identified knowledge, skills, and abilities gaps through specialized role-based training, measuring the impact of the program, and implementing informed program updates using common risks and control weaknesses, and other outputs of the Department's risk management and continuous monitoring activities.

The content of awareness and specialized security training is tailored to the demographics of the Department's workforce. This includes tailoring scenario-based learning activities in all web-based trainings to work-roles and the functions and inputs/outputs of those roles, as well as character development based upon the workforce. The FY 2024 Cybersecurity Symposium was hosted each Thursday in October 2024. This event supports the Department's ability to provide role-based training opportunities to personnel with SSR and develop and maintain a cybersecurity workforce capable of actively reducing and managing risk to ED information and information systems. Over 900 employees and contractors participated in the event. During FY2024 the Department added the Percipio lmmersive Online Platform to the FedTalent Learning Management System. Percipio provides blended learning and improved content search capability for the ED workforce to quickly identify and immerse themselves into activities to support closing competency gaps.

The Department launched and executed three (3) Cybersecurity and Privacy Awareness (CSPA) training courses in FY 2024 providing continual user awareness training; enabling users to define cyber risk management; educating users on identifying and recognizing threats, weaknesses, and

consequences of bad actions; informing users of reporting responsibilities and expectations; and embedding users with knowledge of phishing identification and defense methodologies. The third CSPA course in FY 2024 focused on an introduction to AI, understanding the benefits, and awareness of the potential threat landscape in this emerging and evolving threat area. The course enabled users to gain an awareness of ED policies, knowledge to make informed decisions about using generative AI (GenAI) tools from a risk management perspective, and the strategies for recognizing when bad actors use AI tools.

Building on the successes from prior years, ED continued and expanded the use of badging incentives, presenting users with challenges to model positive behaviors. Since the ED Cybersecurity Training team began awarding badges, other ED programs have followed the model, providing additional opportunities for ED personnel to get involved. To close out the annual cyber badging program for FY 2023, ED awarded the new ED Defender badge to 53 ED employees and contractors as token of appreciation and as recognition for their dedication to protecting the Department against cyber threats by earning at least four badges that fiscal year. In FY 2024, 393 users received the Top Phish Reporter badge for reporting all FY 2023 exercise emails as suspicious and 448 participants received cyber badges for high levels of participation in the October 2023 Symposium. As with prior years, in FY 2024 users were awarded early bird badges for completing mandatory CSPA training within the first thirty days after course launch. 2,498 badges were awarded for FY 2024 CSPA 1, 2,914 badges for FY 2024 CSPA 2, and 2,828 badges for FY 2023 CSPA 3. New in FY 2024, ED awarded badges for early completion of mandatory role-based training with 646 users receiving this new badge.

ED also continued publishing the Training Dashboard; this dashboard visualizes compliance with mandatory training and strengthens the ability of Information System Security Officers (ISSOs) to perform their responsibilities for tracking user compliance. The dashboard enables ISSOs to obtain status information on mandatory awareness and role-based training completions, identify noncompliant users, email noncompliant users, and track and report training information and key metrics.

Each fiscal year ED conducts six (6) simulated phishing exercises targeted all network users. From July 2023 to July 2024, an average of 97.98% of users assessed successfully passed these exercises by properly identifying the email communication as phishing. In May 2024, ED observed one of the highest reporting rates to date, with 57.6% of users reporting the phishing email to the appropriate individuals. During FY 2024 ED conducted a targeted exercise for the Office of the General Counsel centered on AI and partnered with internal POCs for department-wide exercises, such as a privacy-focused exercise conducted in January 2024. In FY 2024, the simulated phishing exercise program maturity was enhanced by integrating the NIST Phish Scale into exercises. The NIST Phish Scale serves as a standardized framework designed to quantify and classify the severity and sophistication of phishing attacks. The Phish Scale uses a rating system that is based on the message content in a phishing email. This can consist of cues that should tip users off about the legitimacy of the email and the premise of the scenario for the target audience, meaning whichever tactics the email uses would be effective for that audience. The Simulated Phishing Program Dashboard used by OCIO IAS and POC Executive Officers, assistant secretaries, and senior leadership was updated and enhanced to increase ease of use and strengthen information provided to Principal Offices. This tool continues to provide visibility

into exercise results, enables the Department to identify and address potential trends through increased awareness outreach and training, and supports ACSD-OCIO-003, *Cybersecurity Awareness Simulated Phishing Exercise Behavioral Based Escalations* requirements. FSA's Enterprise Cybersecurity Group (ECG) designed and implemented updated annual Security and Disclosure Awareness training to all Department employees and contractors who interact with Federal Tax Information (FTI) systems and data. This equipped the entire workforce with the skills and abilities to properly identify, protect, and disclose FTI incidents. This training enabled FSA to receive FTI from the Internal Revenue Services (IRS), which supported the FASFA Simplification Act.

The Department continued to share the maturity of its Cybersecurity Awareness and Training program with other agencies and organizations, collaborating to strengthen cyber training practices; what is notable is that ED, being a small agency, has training and procedures that will help with programs in substantially larger agencies with more personnel and budget funding. The Department's award-winning Cybersecurity and Privacy Awareness Escape Room course was highlighted during a Cybersecurity Awareness, Training, Education, and Research (CATER) Community of Interest (COI) working group sponsored by the Department of Homeland Security, and an overview of the Department's phishing program was shared with the Department of Commerce (DOC). The Social Security Administration (SSA) continued to reach out to the Department and requested meetings to learn more about the Department's program and obtain guidance and direction on how to build and maintain an effective training program. Department personnel also participated with the U.S. Department of Veterans Affairs (VA) to support the development of competencies for cybersecurity workforce roles that will be made available to other agencies in the coming fiscal year.

In May 2024, the Department received recognition and multiple awards from the Federal Information System Security Educator's Association (FISSEA). FISSEA is an organization run by and for Federal government information security professionals to assist Federal agencies in strengthening their employee cybersecurity awareness and training programs. The Department received the FISSEA People's Choice Award in the categories of Awareness Poster, "Beware of Hidden Threats"; Website, "Cybersecurity Symposium 2023 – Get Your Knowledge BoostED"; Cybersecurity Blog, "Cybersecurity Bits and Bytes"; and Training Awareness, "Information Guardians: Immersive Storytelling in Web-based Training".

Information Security Continuous Monitoring

The Information Security Continuous Monitoring (ISCM) Team has been collaborating with internal ED groups (e.g., SAT, Mission Intelligence Visualization System (MIVS), Continuous Diagnostics and Mitigation (CDM), Information System Security Branch (ISSB)) assisting with CDM data validation and defining continuous monitoring activities, metrics, capabilities, and mechanisms for the Department. These activities are captured and outlined in the *Information Security Continuous Monitoring Roadmap* (Version 5.02 published November 17, 2023). The roadmap outlines the Department's strategy for ISCM program implementation and is the core reference for all ISCM related information and provides supporting material for policies, procedures, and standards.

The ISCM played a key role in the Department's effort to address CISA's Binding Operational Directive (BOD) 23-01 and leveraged this directive and internal processes when redesigning the asset inventory (hardware and software) templates and processing for the Department. As a result, the Department has a significantly more detailed view of the assets that make up its IT infrastructure in its official system of record for asset management, GRCT (formerly CSAM). The ISCM team focuses on ensuring the quality of data (most notably, the hardware asset inventory of record for the Department as extracted from GRCT) within the necessary reporting tools to include GRCT, EDCDL, SCRM, and CDM. The ISCM has deployed dashboards within EDCDL to provide automated monitoring of each FISMA boundary with focus on: identified assets; identification of unsupported transport layer security (TLS) or secure socket layer (SSL) protocols and associated identified vulnerabilities; missing and outdated patches needing remediation; data quality metrics (e.g., reported indexes, frequency of ingest, last ingest); unsupported encryption security and technical implementation guide (STIG) compliance with focus on password, data-at-rest (DAR), and data-in-transit (DIT) encryption configurations measured against the latest STIG published by the Department of Defense (DOD) through the DOD Cyber Exchange; and system integration into CDM tools and audit logs into EDCDL.

Incident Response

From an incident response perspective, there has been one major cybersecurity incident across the Department in FY 2024. This major incident was the result of a vendor misusing ED data. ED has also allocated a dedicated resource to work with law enforcement (LE) and the National Cyber Investigative Joint Task Force (NCIJTF). This liaison works collaboratively with ED external and internal stakeholders to enhance the collaborative investigative efforts regarding incident response. As a unique multi-agency cyber center, the NCIJTF has the primary responsibility to coordinate, integrate, and share information to support cyber threat investigations; supply and support intelligence analysis for community decision-makers; and provide value to other ongoing efforts in the fight against the cyber threat to the nation. ED provides direct insight into the education sector from across the K-12, high education, and research and development capabilities to this task force.

Leveraging the Department's new operational Cyber Data Innovation and Services (CDIS) system, dashboards have been built to automate the analysis and review of various aspects of ED audit logs and log sources. For instance, ED has developed and implemented an OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, compliance tracking dashboard to monitor agency event logging (EL1, basic; EL2, intermediate; and EL3, advanced). As directed in M-21-31, ED has prioritized the implementation of all new cybersecurity tools and initiatives by first integrating its high-impact systems and HVAs followed by the remaining FISMA inventory. Progress towards EL1 is consistent, ED now has all FSA servicers, including two HVAs, at a minimum of EL1 reporting.

Cyber Operations holds a weekly threat hunting collaboration meeting with key stakeholders across the enterprise, including FSA, in which indicators of compromise (IOCs), threat methodologies, and top active threats are prioritized and socialized. This includes the integration of an ED intelligence and threat specialist that considers classified, unclassified, and proprietary information for analysis and review activities.

Automated workstreams have been documented and developed in the Department's enterprise ticket system to manage the incident response and reporting processes.

In support of incident response, the FSA team onboarded over 130 new endpoints for the Student Aid and Borrower Eligibility Reform (SABER) initiative and thousands of endpoints from the Next Generation of Loan Servicing under the Unified Servicing and Data Solutions (USDS) initiative. In support of these efforts, we outlined and implemented new data feeds for the newly ingested data. This enabled us to enhance the FSA cybersecurity oversight for FASFA and loan servicing by ensuring the data that the system received were properly monitored, protected and in compliance with OMB M-21-31.

Contingency Planning
ED conducts quarterly Information System Contingency Plan (ISCP) Tabletop Exercise (TTX) activities for system stakeholders to participate. The ED CSF Risk Scorecard v3.0 scores and reports the ongoing compliance with business impact analysis (BIA) completion and annual review; ISCP publication and annual review; ISCP test status; disaster recovery plan (DRP) publication and annual review, as applicable; and DRP test status, as applicable. Further the scorecard provides the capability to continuously monitor – daily, monthly, and quarterly – the status of the contingency planning activities against the Department policies and standards.
In October 2022, FSA expanded its ISCP TTX activities to include a disaster recovery TTX for critical systems. This expansion provides the Department a higher level of assurance that the ISCPs and DRPs will be able to be leveraged if the need arises.

Recommendations
The Department remains committed to addressing the established management challenges in support of remediating the following recommendations.

1.1 : Williams Adley recommends that Chief Information Officer requires the Department and FSA Capture the missing hardware data elements for each identified system and assess whether other information systems may be missing similar or related data elements.

Management's Response: The Department concurs with this recommendation and will continue this effort in FY 2025 and develop a corrective action plan by September 30, 2024.

1.2 : Williams Adley recommends that Chief Information Officer requires the Department and FSA Further define the oversight controls that are in the current policy to ensure all Departmental systems consistently utilize the inventory template when completing/updating the hardware inventory.

Management's Response: The Department concurs with this recommendation and will continue this effort in FY 2025 and develop a corrective action plan by September 30, 2024.

1.3 : Williams Adley recommends that Chief Information Officer requires the Department and FSA Capture the missing software data elements for each identified system and assess whether other information systems may be missing similar or related data elements.

Management's Response: The Department concurs with this recommendation and will continue this effort in FY 2025 and develop a corrective action plan by September 30, 2024.

1.4 : Williams Adley recommends that Chief Information Officer requires the Department and FSA Further define the oversight controls that are in the current policy to ensure all Departmental systems consistently utilize the inventory template when completing/updating the software inventory.

Management's Response: The Department concurs with this recommendation and will continue this effort in FY 2025 and develop a corrective action plan by September 30, 2024.

2.1 : Williams Adley recommends that Chief Information Officer requires the Department to Implement a process to monitor that PRDs are reviewed and signed prior to the security investigation.

Management's Response: The Department concurs with this recommendation and will continue this effort in FY 2025 and develop a corrective action plan by September 30, 2024.

2.2 : Williams Adley recommends that Chief Information Officer requires the Department to Implement automation process to centrally document, track, and share risk designation and screening information.

Management's Response: The Department concurs with this recommendation and will continue this effort in FY 2025 and develop a corrective action plan by September 30, 2024.

2.3 : Williams Adley recommends that Chief Information Officer requires the Department to Reinforce their process for documenting the authorization, review, and approval of PUAs.

Management's Response: The Department concurs with this recommendation and will continue this effort in FY 2025 and develop a corrective action plan by September 30, 2024.

2.4 : Williams Adley recommends that Chief Information Officer requires the Department to Develop enhanced monitoring controls to ensure proper internal controls mechanisms and processes are strictly enforced.

Management's Response: The Department concurs with this recommendation and will continue this effort in FY 2025 and develop a corrective action plan by September 30, 2024.

2.5 : Williams Adley recommends that the Chief Information Officer require and make Departmental Principal Offices to re-evaluate the use of PIV alternates/exemptions across the organization, and modify onboarding procedures, as needed, to be fully compliant with HSPD-12[20] in accordance with a new strategic directive.

[20] Based on the structure of the Department and its various offices, this recommendation may require a unified effort across multiple principal offices to ensure that the Department's onboarding processes support the requirements of HSPD-12.

Management's Response: The Department concurs with this recommendation and will continue this effort in FY 2025 and develop a corrective action plan by September 30, 2024.

3.1 : Williams Adley recommends that the Chief Information Officer require the Department and FSA to review and approve the USDS-MaxED/AidVntge and EDAWSEW MOU. Furthermore, the Department and FSA should update existing procedures and ensure all MOUs reflect the appropriate two-year review cycle.

Management's Response: The Department concurs with this recommendation and will continue this effort in FY 2025 and develop a corrective action plan by September 30, 2024.

Thank you for the opportunity to comment on this draft report and for your continued support of the Department and its critical mission. If you have any questions regarding this matter, please contact the Chief Information Security Officer, Steven Hernandez at (202) 245-7779.

cc: Gary Stevens, Deputy Chief Information Officer, Office of the Chief Information Officer
Steven Hernandez, Director, Information Assurance Services, Office of the Chief Information Officer
Margaret Glick, FSA Chief Information Officer, Federal Student Aid
Dan Commons, FSA Deputy Chief Information Officer, Federal Student Aid
Davon Tyler, FSA Chief Information Security Officer, Federal Student Aid
Sam Rodeheaver, Audit Liaison, Office of the Chief Information Officer
Stefanie Clay, Audit Liaison, Federal Student Aid
Bucky Methfessel, Senior Counsel for Information & Technology, Office of the General Counsel
April Bolton-Smith, Post Audit Group, Office of the Chief Financial Officer
L'Wanda Rosemond, AARTS Administrator, Office of Inspector General
Kevin Herms, Senior Agency Official for Privacy, Office of Planning, Evaluation and Policy Development

Appendix E. FY 2024 Conditions, Associated Criteria, and Recommendation Issued

#	FISMA Metric Domain	Condition Description	Associated Criteria	Recommendation Issued
1	Risk Management	The Department and the FSA did not consistently capture standard data elements/taxonomy for managing hardware inventory for two of its information systems. Specifically, Williams Adley found that the following data elements were missing within the respective system's hardware inventory: • Enterprise Technology Services – Integrated Services Systems (ETS-ISS): Manufacturer Serial Number, and Date Device Added to System Boundary; and • Unified Servicing and Data Solution – Maximus Education/Aidvantage (USDS-EDF): Active Directory (AD) Domain, Manufacturer Serial Number, Basic Input/Output System (BIOS) Universal Unique Identifier/Globally Unique Identifier (UUID/GUID) and Media Access Control	The Information Technology (IT) System Configuration Management (CM) Standard, dated February 10, 2023, states: • CM-8 System Component Inventory (L, M, H and Control Overlay) o Develop and document an inventory of system components that: ▪ Accurately reflects the system; ▪ Includes all components within the system; ▪ Does not include duplicate accounting of components or components assigned to any other system; ▪ Is at the level of granularity deemed necessary for	Williams Adley recommends that the Chief Information Officer require the Department and FSA to: • Capture the missing hardware data elements for each identified system and assess whether other information systems may be missing similar or related data elements (Recommendation 1.1). • Develop oversight controls to ensure all Departmental systems utilize the inventory template when completing/updating the hardware inventory (Recommendation 1.2).

		(MAC) Address, and Date Device Added to System Boundary.	tracking and reporting; and • Includes the following information to achieve system component accountability: as defined in CSAM System Information, Appendix S – Hardware Listing and System Information, Appendix T – Software Listing; not required for cloud service providers or Shared Services.	
2	Risk Management	The Department did not consistently capture standard data elements/taxonomy for managing software inventory for its systems. Specifically, Williams Adley found that the following data elements were missing within the respective system's software inventory: • Enterprise Technology Services – Integrated Services Systems (ETS-ISS): Software Common Platform Enumeration (CPE) ID, Critical Software, Software/Database Vendor, License, License Expiration, Date Software Added to Inventory, Function, Environment, Hostname/Host ID, Date Software was First Detected on Device, Software Component Owner, Software Administrator, and First Tier Supplier • Education Security Tracking and Reporting System (EDSTAR): Date Software Added to Inventory, Hostname/Host ID, Date Software was First Detected on Device, and First Tier Supplier		Williams Adley recommends that the Chief Information Officer require the Department and FSA to: • Capture the missing software data elements for each identified system and assess whether other information systems may be missing similar or related data elements (Recommendation 1.3). • Develop oversight controls to ensure all Departmental systems utilize the inventory template when completing/updating the software inventory (Recommendation 1.4).

		• Unified Servicing and Data Solution – Maximus Education/Aidvantage (USDS-MaxEd/AidVntge): License Expiration • Unified Servicing and Data Solution – EDFinancial (USDS-EDF): Software CPE ID and Critical Software, Serial/License, Function, Environment, Software Host, Hostname/Host ID, Date Software was First Detected on Device, and First Tier Supplier.		
3	Contingency Planning	The MOU between the USDS-MaxED/AidVntge and EDAWSEW was last reviewed/updated on June 16, 2022.	The MOU between USDS-MaxED/AidVntge and EDAWSEW, dated June 16, 2022, states that the "MOU should be reviewed by the Information System Security Officer (ISSO) at least every year and/or whenever a major system change occurs". Furthermore, any significant changes that affect the agreement "should be identified and shared between the signatories to ensure the MOU is updated, re-signed, and uploaded to appropriate CSAM records by the Information System Owner (ISO)/ISSO".	Williams Adley recommends that the Chief Information Officer require the Department and FSA to review and approve the USDS-MaxED/AidVntge and EDAWSEW MOU. Furthermore, the Department and FSA should update existing procedures and develop additional measures to ensure all MOUs reflect the appropriate two-year review cycle (Recommendation 3.1).
4	Identity and Access Management	Williams Adley identified the following issues related to the Department and Federal Student Aid (FSA)'s process supporting the	According to control PS-02 within the Information Technology (IT) Personal Security (PS) document, dated December 15, 2023, the Department	Williams Adley recommends that the Chief Information Officer require the Department and FSA to:

		review and approval of personnel PRDs: • Five (5) out of 22 PRDs sampled were signed after the investigation date; and • The Department and FSA do not have an automated process to centrally document, track, and share risk designation and screening information.	and FSA are required to: • Assign a risk designation to all organizational positions; • Establish screening criteria for individuals filling those positions; and • Review and update position risk designations: o Every five years for federal employees; and o During contract solicitation for contractors in accordance with Administrative Communication System Directive (ACSD) - Office of Finance and Operations (OFO)-013, Contractor Employee Personnel Security Screenings. Furthermore, control PS-03 within the IT PS document requires the Department to: • Screen individuals prior to authorizing access to the system; and • Rescreen individuals in accordance with requirements specified in ACSD-OFO-017 Federal Employee Personnel	• Implement an enhanced process to monitor that PRDs are review and signed prior to the security investigation (Recommendation 2.1); and • Implement automation processes to centrally document, track, and share risk designation and screening information (Recommendation 2.2).

			Security Screening and ACSD-OFO-013 Contractor Employee Personnel Security Screenings. • The FISMA Inspector General (IG) Metric requires that the organization employs automated mechanisms to test system contingency plans more thoroughly and effectively.	
5	Identity and Access Management	The Department and the Federal Student Aid (FSA) did not consistently maintain the segregation of duties supporting the PUA process. Specifically, for two (2) sampled privileged accounts, the creator/requestor and approver of the access request were the same person	The Information Technology (IT) Access Control (AC) Standard, dated February 9, 2024, requires that authorize access to the system should be based on: • A valid access authorization; • Intended system usage; and • Requested roles/privileges. The National Institute of Standards & Technology (NIST) Special Publication (SP) AC-5 control states that: Separation on of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions.	Williams Adley recommends that the Chief Information Officer require the Department and FSA to: • Reinforce their process for documenting the authorization, review, and approval of PUAs (Recommendation 2.3). • Develop enhanced monitoring controls to ensure proper internal controls mechanisms and processes are strictly enforced (Recommendation 2.4).
6	Identity and Access Management	Williams Adley identified the following issues related to implementation of the Department	The Information Technology (IT) Identity and Authentication (IA) Standard, dated September 22, 2023,	Williams Adley recommends that the Chief Information Officer require and make

		and the Federal Student Aid (FSA)'s PIV exemption users: • The Department continued to deploy PIV-Alternative (ALT) configured GFEs to the Department users. • 34 Department and FSA users were granted a short-term PIV-exemption for more than three (3) times. • 860 Department users were granted long-term PIV-Exemption prior to the process requiring submission for long-term PIV-Exemption extension request form. • For 40 Department and FSA users, the respective Principal Offices (POs) did not complete and submit the required long-term PIV-Exemption extension request forms.	identified requirement within the Control Overlay IA-2(12) ED-01 (L, M, H) to use Homeland Security Presential Directive (HSPD)-12 compliant PIV (including Derived PIV) as the "primary" means of authentication to Federal information systems. The Department Standard PR.AC: "Emergency PIV Alternative" Memorandum states effective sixty days from the issuance of this memorandum, April 14, 2022, "all federal employees, and contractors are required to use a PIV smartcard (badge) for authentication and access to Federal facilities and IT systems." The "Emergency PIV Alternative" Memorandum also requires that the Department continues performing progressive communication escalation procedures with personnel identified as still using: PIV – Alternate Multi-factor Authentication (MFA). Federal employees and contractors using a government furnished laptop configured to authenticate without a PIV card must also submit a request in ServiceNow to convert the laptop to the standard PIV authentication configuration. In conjunction with this memorandum, within sixty days, OCIO	Departmental Principal Offices to re-evaluate the use of PIV alternates/exemptions across the organization, and modify onboarding procedures, as needed, as needed, to be fully compliant HSPD-12 in accordance with a new strategic direction (Recommendation 2.5).

			will stop deploying laptops with PIV-Alternate configuration.	