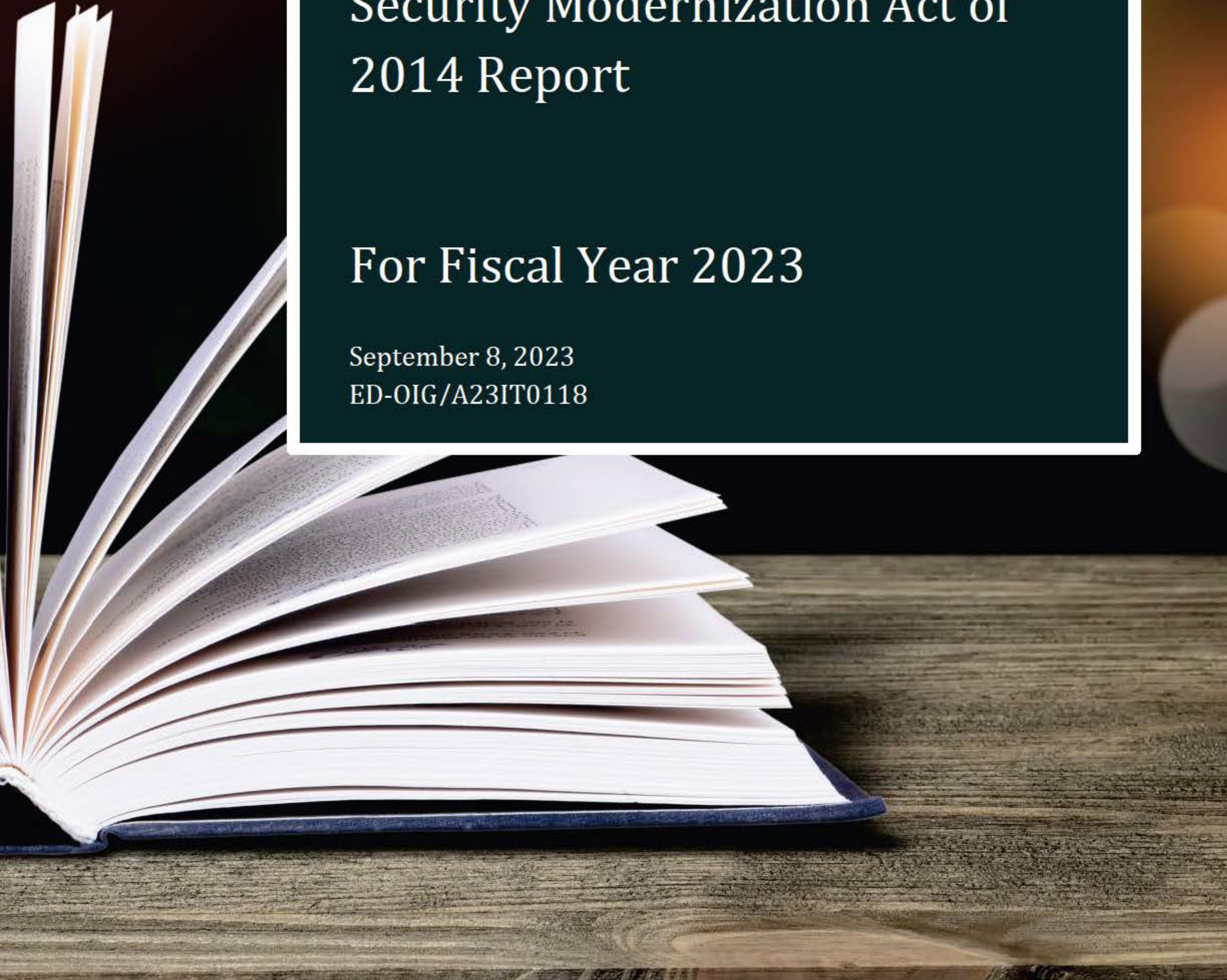
U.S. Department of Education
Office of Inspector General

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

For Fiscal Year 2023

September 8, 2023
ED-OIG/A23IT0118



UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

September 8, 2023

Memorandum

TO: Luis Lopez
Chief Information Officer
Office of the Chief Information Officer

FROM: Kevin J. Young //SIGNED//
Assistant Inspector General
Technology Services
Office of Inspector General

SUBJECT: Final Audit Report
Federal Information Security Modernization Act of 2014 Audit of the United States Department of Education's Information Security Program and Practices for Fiscal Year 2023
Control Number ED-OIG/A23IT0118

Attached is the **final audit report** that determined whether the Department's 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, 2022, to June 30, 2023.

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, monitored the performance of the audit, reviewed contractor audit documentation, attended critical meetings with the Department officials and reviewed the contractor's audit controls. The review was designed to help ensure that

- the audit complied with GAGAS and other OIG policies and procedures;
- contract requirements regarding objectives, scope, and methodology were being met;
- bi-weekly status meeting to discuss whether milestones were being met; and
- draft and final report reviews conducted by the OIG Information Technology Audits Division provided the assurance that the contractor's work can be relied on.

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 October 31, 2023.

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.

Enclosure

cc: Cindy Marten, Deputy Secretary, Office of the Secretary and Deputy Secretary
James Kvaal, Under Secretary, Office of the Under Secretary
Richard Cordray, 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
Phil Rosenfelt, Deputy General Counsel, Office of General Counsel
Antonio Murray, Deputy Assistant Inspector General, Technology Services
Joseph Maranto, Director, Information Technology Audits, Technology Services
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

WILLIAMS
ADLEY

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 2023

September 8, 2023

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 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.

W LL AMS
ADLEY

Mr. Luis Lopez
Chief Information Officer
Office of the Chief Information Officer
400 Maryland Avenue, SW
Washington, DC 20202

Dear Mr. Lopez:

We are pleased to provide our report outlining the results of the performance audit conducted to determine the effectiveness of the Department of Education's information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) for the fiscal year (FY) 2023 audit.

On December 2, 2022, the Office of Management and Budget (OMB) issued Memorandum M-23-03 ("Memorandum for the Heads of Executive Departments and Agencies: Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements") to provide instructions for meeting the FY 2023 FISMA reporting requirements.

To achieve this objective, we reviewed the FISMA security 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 2023 audit provides a reasonable basis for our conclusions and maturity ratings.

Based on the results of the audit procedures performed for the FY 2023 audit period, Williams Adley concluded that the Department of Education (Department) has met the requirements to be operating at an effective level of security outlined within the FY 2023 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 appendix. 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.

//SIGNED//

September 8, 2023

Table of Contents

Results in Brief

The objective of the Fiscal Year (FY) 2023 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.

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 20 core and 20 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 previous year's audit.[3]

At the conclusion of the FY 2023 audit, Williams Adley determined that the Department's overall IT security program and practices are effective as eight out of the nine FISMA domains met the requirements needed to operate at a Level 4 maturity rating[4].

Additionally, Williams Adley identified a total of 12 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 section of this report outlines the individual scores for each metric question evaluated and any conditions identified.

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

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

[2] For the FY 2023 FISMA audit, Williams Adley selected (b) (7) (e) 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.

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	3.50
Recover	Contingency Planning	Managed and Measurable	4.00

Table 1 - FY 2023 Core Maturity Ratings

Function	Domain	Maturity Rating	Calculated Average
Identify	Risk Management	Managed and Measurable	4.33
Identify	Supply Chain Risk Management	Managed and Measurable	4.00
Protect	Configuration Management	Managed and Measurable	3.67
Protect	Identity and Access Management	Consistently Implemented	3.50
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 2023 Supplemental Maturity Ratings

Williams Adley also followed up on the status of the 30 recommendations issued during the last three FISMA audits (FY 2019 through FY 2021) and one FISMA evaluation (FY 2022) to determine whether the Department had implemented their proposed corrective actions. Overall, Williams Adley determined that four prior year recommendations remain open, as of the end of the fieldwork phase. The status of each recommendation is listed in Appendix B, Status of Prior-Year Recommendations along with the proposed target action date for all open recommendations. 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 20 core and 20 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, 2023.

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 2023 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.

The Department's OCIO advises and assists the Secretary and other senior officers in acquiring information technology (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[5].

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 security programs. Additionally, the Act established that the OMB is responsible for submitting an annual

[5] The Department's FY 2023 total spending for IT investments was estimated at $1.26 billion, which included $884 million in spending on major IT investments (70 percent of total spending).

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.

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. FISMA states that the independent evaluation is to be performed by the agency Office of Inspector General (OIG) or an independent external auditor. 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 2, 2022, the OMB issued Memorandum M-23-03 ("Memorandum for the Heads of Executive Departments and Agencies: Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements") to provide instructions for meeting the FY 2023 FISMA reporting requirements.

According to the memorandum, the FY 2023 reporting period presents the first opportunity for an agency Inspector General or independent assessor to evaluate the following group of metrics:

- Core Metrics – Metrics that are assessed annually and represent a combination of Administration priorities, high impact security processes, and essential functions necessary to determine security program effectiveness.
- Supplemental Metrics – Metrics that are assessed at least once every two years and represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.

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.

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 2023 Audit Results

Williams Adley assessed the effectiveness of the Department of Education (Department)'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 Fiscal Year (FY) 2023 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 2023 Maturity Rating	FY 2022 Maturity Rating
1	Comprehensive and accurate inventory of agency information systems	Level 4	Level 3
2	An up-to-date inventory of hardware assets	Level 4	Level 3
3	An up-to-date inventory of software and associated licenses	Level 4	Level 3
5	Information system security risks are adequately managed at all organization tiers	Level 4	Level 4
10	Use technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities	Level 4	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 4.00 and a maturity rating of Level 4 (Managed and Measurable)[6].

Risk Management – Supplemental Reporting Metrics

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

The OMB identified three (3) supplemental reporting metrics for evaluation in FY 2023, as outlined in ***Table 5***:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2021 Maturity Rating[7]
7	Roles and responsibilities of internal and external stakeholders	Level 4	Level 3
8	Plans of action and milestones (POA&Ms) are used to effectively mitigate security weaknesses	Level 4	Level 3
9	Information about cybersecurity risks is communicated in a timely and effective manner to appropriate internal and external stakeholders	Level 5	Level 5

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 4.33 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 increased from Level 3 to Level 4 (Managed and Measurable). Williams Adley found that the Department has continued 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[8]. In addition, the Department is in the process of remediating FY 2020 open recommendation 1.4 related to the use of automation to ensure all Department-wide IT inventories are accurate, complete, and periodically tested for accuracy with a target date of September 30, 2024.

Williams Adley concluded that the maturity of FISMA metric question 2 increased from Level 3 to Level 4 (Managed and Measurable). Williams Adley found that the Department has an organization-wide hardware asset management capability, and its hardware assets are subject to the Department's ISCM strategy. Williams Adley [redacted] (b) (7) (e) Condition 1). This condition was deemed low risk as both systems are managed by external parties and subject to the Department's supply chain risk management processes. As a result, Williams Adley will not issue a recommendation to address this condition.

Williams Adley concluded that the maturity of FISMA metric question 3 increased from Level 3 to Level 4 (Managed and Measurable). 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. Williams Adley did identify a low-risk issue related

[7] The FY 2023 supplemental FISMA reporting metrics were last evaluated during the FY 2021 reporting period.

[8] Within the context of the FY 2023 FISMA audit, the Department's ISCM program was deemed effective.

to missing serial ID, license number, and license expiration data fields required by its standard data elements/taxonomy for the following systems (Condition 2):

(b) (7) (e)

This condition has minimal impact on the Department's maturity as the Department has already identified the issue and created a POA&M to address the root cause. As a result, Williams Adley will not issue a recommendation to address this condition.

Williams Adley determined that FISMA metric question 5 remains at Level 4 (Managed and Measurable). However, Williams Adley identified the following minor issues related to the inconsistent implementation of defined activities for managing information system security risks at all organization tiers:

- (β) (7) (ε) Review Checklist was not signed by the Information System Owner (ISO) and Information System Security Officer (ISSO). (Condition 3)
- (b) (7) (e) Review Checklist was not performed annually, last updated February 11, 2021. (Condition 4)
- (b) (7) (e) Security Assessment Report (SAR) included in the system's Authorization to Operate (ATO) package did not demonstrate the results of the most recent assessment. (Condition 5)
- (b) (7) (SAR included in the system's ATO package did not demonstrate the results of the most recent assessment. (Condition 6)

These conditions were considered to be low risk as the Department has performed the associated control activities but did not upload the correct documentation to its system or record, Cyber Security Assessment and Management System (CSAM), in a timely manner.

Williams Adley concluded that the maturity of FISMA metric question 7 increased from Level 3 to Level 4 (Managed and Measurable) based on the results of testing across the core and supplemental metrics demonstrating that risk management stakeholders are performing their defined roles and responsibilities.

Williams Adley identified an increase in the maturity for FISMA metric question 8 from Level 3 to Level 4 (Managed and Measurable) as the Department monitored and analyzed qualitative and quantitative performance measures on the effectiveness of its POA&M activities and used that information to make appropriate adjustments, as needed, to ensure that its risk posture is maintained.

Williams Adley determined that FISMA metric question 9 remains at Level 5 (Optimized) as the Department has incorporated cybersecurity risk management into its enterprise risk management program reporting tool.

Williams Adley determined that FISMA metric question 10 remains at Level 4 (Managed and Measurable) as the Department has integrated cybersecurity risk management into the enterprise risk management reporting processes.

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

Cause, Effect, and Recommendations

Williams Adley believes that conditions 3, 4, 5, and 6 identified within the risk management and information security continuous monitoring domains are a result of the Department and Federal Student Aid (FSA) not consistently overseeing the process of reviewing and approving SSP Review Checklists and SARs prior to being uploaded in the system of record, CSAM. Without a timely and accurate review of the content of system authorization packages, the Department is not be able to effectively implement the ongoing authorization and monitoring processes and to ensure risks are identified and monitored. To address conditions 3, 4, 5, and 6, and their associated root cause, Williams Adley recommends that the Chief Information Officer requires the Department and FSA to:

- Take immediate corrective actions to implement enhanced monitoring procedures to allow for timely review of system authorization packages and appropriate authorization prior to submission into CSAM (Recommendation 1.1).

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***:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2022 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 4	Level 3

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 4.00 and a maturity rating of Level 4 (Managed and Measurable).

Supply Chain Risk Management – Supplemental Reporting Metrics

The OMB identified two supplemental reporting metrics for evaluation in FY 2023, as outlined in ***Table 7***:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2021 Maturity Rating
12	Agency wide supply chain risk management strategy to manage supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services	Level 4	Level 2
13	The agency ensures that products, system components, systems, and services of external providers are consistent with cybersecurity and supply	Level 4	Level 2

	chain requirements.		

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 for FISMA metric question 12 from Level 2 to Level 4 (Managed and Measurable) as the Department implemented its defined activities related to the management supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services. Furthermore, the Department utilizes qualitative and quantitative performance metrics to monitor the information security and supply chain risk management performance of external providers.

Williams Adley identified an increase in the maturity for FISMA metric question 13 from Level 2 to Level 4 (Managed and Measurable) as the Department implemented its defined activities to ensure that products, system components, systems, and services of external providers are consistent with cybersecurity and supply chain requirements. Furthermore, the Department utilizes qualitative and quantitative performance metrics to monitor the information security and supply chain risk management performance of external providers.

Williams Adley identified an increase in the maturity for FISMA metric question 14 from Level 3 to Level 4 (Managed and Measurable) as the Department consistently implemented 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, Williams Adley identified that the supply chain risk management governing documents were outdated and required annual revision. Williams Adley brought this finding to the attention of the Department and as of June 28, 2023, the supply chain risk management governing documents were updated to address identified finding[9].

Cause, Effect, and Recommendations

Williams Adley did not identify any issues 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 that not all security domains within the Protect function 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 software versions and updates installed

[9] Williams Adley will not issue a recommendation for the preliminary finding related to the supply chain risk management's governing documents as the Department made corrective actions within the audit period.

on the organization’s computer systems.

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 2023 Maturity Rating	FY 2022 Maturity Rating
20	Use of configuration settings and common secure configurations	Level 4	Level 4
21	Use of flaw remediation processes	Level 4	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 4.00 and a maturity rating of Level 4 (Managed and Measurable).

Configuration Management – Supplemental Reporting Metrics

The OMB identified three supplemental reporting metrics for evaluation in FY 2023, as outlined in ***Table 9*:**

Metric Question	Topic	FY 2023 Maturity Rating	FY 2021 Maturity Rating
19	Use of baseline configurations	Level 4	Level 3
22	Adoption of the Trusted Internet Connection (TIC) 3.0 program to assist in protecting the agency’s network	Level 3	Level 2
24	Use of a vulnerability disclosure policy (VDP) as part of its vulnerability management program	Level 4	Level 2

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 3.67 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 19 from Level 3 to Level 4 (Managed and Measurable) as the Department utilizes automated mechanisms to detect unauthorized hardware, software, and firmware within its environment. Williams Adley also identified two conditions related to the governing documents supporting the Department’s configuration management program:

- (β) (7) (ε) SSPs referring to a rescinded/retired Baseline Standard within the control implementation statements for minimum security controls (Condition 8).

- The Software Management and Acquisition Policy, last updated on April 10, 2019, requires annual revision (Condition 7).

Although Williams Adley identified issues related to the Department's governing documents, the Department was able to not only consistently implement its defined processes but were managing and measuring the effects as well.

Williams Adley determined that FISMA metric question 20 remains at Level 4 (Managed and Measurable) as the Department employs automation to maintain its common secure configurations. Additionally, Williams Adley performed a vulnerability assessment and penetration test to determine the effectiveness of the Department's security practices and no significant issues were identified. Lastly, Williams Adley confirmed that the Department is in process of remediating FY 2022 open recommendation 1.2 related to the establishment of additional oversight controls to update, remove, or replace obsolete or unsupported solutions and encryption protocols. Refer to Appendix B for additional details.

Williams Adley determined that FISMA metric question 21 remains at Level 4 (Managed and Measurable) as the Department centrally manages its flaw remediation processes and utilizes automation to ensure that patches are applied, as needed. Furthermore, the Department utilizes qualitative and quantitative performance metrics to monitor the effectiveness of its flaw remediation processes.

Additionally, Williams Adley found that Vulnerability Management Standard Operating Procedures (SOP) was outdated and referred to the rescinded and retired Baseline Standard within the document. However, per follow up with the Department and obtaining the latest version of the SOP updated as of June 26, 2023, Williams Adley identified that the Department had begun updating the SOP in January 2023 and due to unexpected resource constraints finalized on June 26, 2023. Therefore, Williams Adley determined that the initially identified issue was resolved and did not warrant a finding nor a recommendation.

Lastly, Williams Adley confirmed that the Department is in the process of implementing the corrective actions identified to address FY 2022 open recommendation 1.1 related to the prioritization of patches and their application within established timeframes. Refer to Appendix B for additional details.

Williams Adley identified an increase in the maturity for FISMA metric question 22 from Level 2 to Level 3 (Consistently Implemented) as the Department has made improvements to its configuration management program to meet the TIC requirements outlined within Office of Management and Budget (OMB) Memorandum (M) 19-26 since FY 2021, when the FISMA metric 22 was last evaluated. Specifically, the Department funded and started the migration its users from its legacy virtual private network (VPN) to a secure access service edge (SASE) architecture and created automated playbooks within its Security Orchestration Automation & Response (SOAR) solution to improve the efficiency of its security operations. Based on the most recent Technology Modernization Fund update in May 2023, the Department expects to migrate approximately 35% of its systems behind SASE by the second half of calendar year 2023. Additionally, the Department is in process of improving its maturity across all Zero Trust Pillars.

Additionally, Williams Adley determined that the Department is making significant progress to remediate the FY 2019 open recommendation 2.4 related to ensuring that websites are routed through a trusted internet connection. As of the conclusion of the FY 2023 FISMA audit, the Department only has [redacted] TIC non-compliant websites remaining from the 51 identified in FY 2019. Once remediated and resolved, the Department will be able to fully monitor and review the implemented TIC 3.0 use cases to determine effectiveness and incorporates new/different use cases, as appropriate.

Lastly, Williams Adley identified an increase in the maturity for FISMA metric question 24 from Level 3 to Level 4 (Managed and Measurable) as the Department has integrated its VDP with its existing vulnerability management processes.

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

Cause, Effect, and Recommendations

Williams Adley believes that condition 7 identified within the configuration management domain is the result of the Department not consistently overseeing the process of reviewing and approving the policy on an annual basis. Without a timely and accurate review of the policy, the Department may not execute the appropriate process for purchasing and managing its software assets. To address condition 7 and its associated root cause, Williams Adley recommends that Chief Information Officer requires the Department to:

- Develop and implement an effective quality control review process for its policies and procedures. (Recommendation 3.1)

The root cause and effect for condition 8 are the same as conditions 3, 4, 5, and 6 identified within the Risk Management domain. As a result, Recommendation 1.1 also applies to condition 8. Refer to the Identify Section of the FY 2023 Audit Results for additional details.

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 2023 Maturity Rating	FY 2022 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 Identity Assurance Level (IAL)3/Authenticator Assurance Level (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 2	Level 3

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 3.00 and a maturity rating of Level 3 (Consistently Implemented).

Identity and Access Management – Supplemental Reporting Metrics

The OMB identified four (4) supplemental reporting metrics for evaluation in FY 2023, as outlined in ***Table 11***:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2021 Maturity Rating
26	Roles and responsibilities of identity, credential, and access management (ICAM) stakeholders	Level 3	Level 2
27	Comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities	Level 3	Level 2
29	Access agreements for individuals (both privileged and nonprivileged users) that access its systems are completed and maintained	Level 4	Level 4
33	Configuration and connection requirements are maintained for remote access connections	Level 4	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 3.50 and a maturity rating of Level 3 (Consistently Implemented).

Metric Question Maturity Descriptions

Williams Adley identified an increase in the maturity for FISMA metric question 26 from Level 2 to Level 3 (Consistently Implemented) as ICAM stakeholders are mostly performing their identity and access management roles and responsibilities. However, the issues identified in FISMA metric questions 27, 30, and 32 indicate that the IAM activities are not performed effectively as intended.

Williams Adley identified an increase in the maturity for FISMA metric question 27 from Level 2 to Level 3 (Consistently Implemented) as the Department implemented its defined ICAM policy, strategy, process, and technology solution road map.

Williams Adley determined that FISMA metric question 29 remains at a Level 4 (Managed and Measurable) maturity as the Department uses automation to manage and review user access agreements for privileged and non-privileged users.

Williams Adley determined that FISMA metric question 30 remains at a Level 3 (Consistently Implemented) maturity as the (b) (7) (e) For system level access, the Department has implemented multifactor authentication.

Williams Adley determined that FISMA metric question 31 remains at a Level 4 (Managed and Measurable) maturity as the Department has implemented security controls that require privileged users, including those who can make changes to DNS records, to use strong authentication mechanisms when authenticating to Department systems.

Williams Adley identified a drop in maturity for FISMA metric question 32 to Level 2 (Defined) due to the inconsistent implementation of processes for provisioning, managing, and reviewing privileged accounts. Specifically, Williams Adley found issues related to the implementation of its access provisioning controls for the following systems' privileged users:

- All three sampled (b) (7) (e) users did not complete elevated access request form.
- Two out of three sampled (b) (7) (e) users did not complete elevated access request form.
- One out of three sampled (b) (7) (e) user did not complete any onboarding forms, including an elevated access request form.
- All eight sampled (b) (7) (e) users did not complete any onboarding forms, including an elevated access request form. (Condition 10)

In addition, the Department and FSA are not compliant with the Event Logging (EL)1 and EL2 requirements, at the enterprise-level, as established within OMB Memorandum (M)-21-31 (Condition 11).

Williams Adley identified an increase in the maturity for FISMA metric question 33 from Level 2 to Level 4 (Managed and Measurable) as the Department ensured that end user devices were appropriately configured prior to allowing remote access and restricted the ability of individuals to transfer data accessed remotely to non-authorized devices.

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

Cause, Effect, and Recommendations

Williams Adley believes that condition 9 identified within the identity and access management domain is the result of the Department and FSA encountering technical limitations to provide network access to users that have either have no PIV cards or PIV card issues. The continued use of the less secure form of authentication results in a greater risk of an account becoming compromised, and the Department's network being exposed to unauthorized users, which could result in compromising the confidentiality, integrity, and availability of information systems. To address condition 9 and its associated root cause, Williams Adley recommends that the Chief Information Officer requires the Department and FSA to:

- Take immediate corrective actions to remove users from PIV exempt list. (Recommendation 4.1)

Williams Adley believes that condition 10 identified within the identity and access management domain is the result of the Department did not establish a process for the completion and maintenance of privileged user onboarding, and elevated user access forms to obtain privileged access. Furthermore, the Department has neither formally developed, nor implemented an effective quality control review process, to ensure that forms are completed, tracked, and properly maintained for records. Without an effective process for the completion and maintenance of user onboarding, elevated and non-elevated user access forms, the Department cannot ensure that employees are complying with Departmental policy and procedure and did not allow the Department to verify whether the appropriate access was granted, and IT asset were safeguarded. To address condition 10 and its associated root cause, Williams Adley recommends that the Chief Information Officer requires 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. (Recommendation 4.2)

Williams Adley believes that condition 11 identified within the identity and access management and incident response domain is the result of the lack of funding and resources to implement the required EL1 and EL2 maturity capabilities at the enterprise level, although the Department deployed some of EL1 functionalities at the system level. Without the full implementation of EL1 and EL2 capabilities, the Department cannot ensure full monitoring and the visualization of hardware and software assets. Williams Adley recommends that the Chief Information Officer require that the Department and FSA:

- 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. (Recommendation 4.3)

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 2023 Maturity Rating	FY 2022 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 2
37	Use of security controls to prevent data exfiltration and enhance network defenses	Level 4	Level 3

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 one supplemental reporting metric for evaluation in FY 2023, as outlined in ***Table 13***:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2021 Maturity Rating
35	Privacy program for the protection of personally identifiable information (PII) that is collected, used,	Level 4	Level 2

	maintained, shared, and disposed of by information systems		

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 identified an increase in the maturity for FISMA metric question 35 from Level 2 to Level 4 (Managed and Measurable) as the Department has implemented its privacy program and utilizes quantitively and qualitative performance measures to evaluate the effectiveness of its privacy activities. Williams Adley also identified that the Department did not review and update its (b) (7) (e) Privacy Impact Assessment (PIA) within its required two-year cycle. (Condition 12)

Williams Adley identified an increase in the maturity for FISMA metric question 36 from Level 2 to Level 4 (Managed and Measurable) as the Department has implemented security controls to protect its PII and other sensitive information. Williams Adley also determined that the Department remediated and resolved FY 2022 recommendation 3.1 related to the implementation of monitoring and oversight controls to ensure media sanitization policies and processes are in place and document evidence of the disposal or reuse of all used digital media. Refer to Appendix B for additional details.

Williams Adley identified an increase in the maturity for FISMA metric question 37 from Level 3 to Level 4 (Managed and Measurable) as the Department analyzes qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses. Williams Adley also determined that the Department remediated and resolved FY 2022 recommendation 1.2 related to the establishment of additional oversight controls to update, remove, or replace obsolete or unsupported solutions and encryption protocols. Refer to Appendix B for additional details.

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

Cause, Effect, and Recommendations

Per discussion with the Department, Williams Adley was informed that condition 12 occurred due to a decision made by Management to prioritize privacy risk management over its two-year deadline as statutory changes impacted their privacy program and subsequently impacted the timely update of the (b) (7) (e) Williams Adley concluded that this condition is low risk as the Department was in process of completing the PIA at the completion of the fieldwork phase. However, by not completing the update within the two-year period, the Department is non-compliant with its own established policy. By not documenting, validating, and maintaining PIAs within the required time frame, the Department may not be able to determine how information is handled to ensures compliance with applicable legal, regulatory, and policy requirements regarding privacy; determine the risks and effects of collecting, maintaining, and disseminating information; and examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks, in a timely manner. To address condition 12 and its associated root cause, Williams Adley recommends that the Chief Information Officer requires the Department to:

- Update Department PIA processes, quality control procedures, and monitoring controls to validate, track, and enforce the timely completion and review of PIAs (Recommendation 5.1).

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. For example, we judgmentally selected a sample of 23 new user accounts and verified that security training was completed.

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 2023 Maturity Rating	FY 2022 Maturity Rating
42	Use of assessments of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training	Level 4	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 4.00 and a maturity rating of Level 4 (Managed and Measurable).

Security Training – Supplemental Reporting Metrics

The OMB identified two supplemental reporting metrics for evaluation in FY 2023, as outlined in **Table 15**:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2021 Maturity Rating
41	Roles and responsibilities of security awareness and training stakeholders	Level 4	Level 3
43	Use of security awareness and training strategy/plan	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 determined that FISMA metric question 41 is operating at a Level 4 (Managed and

Measurable) maturity as the Department's resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to consistently implement security awareness and training responsibilities. Furthermore, stakeholders are held accountable for carrying out their roles and responsibilities effectively.

Williams Adley determined that FISMA metric question 42 is operating at a Level 4 (Managed and Measurable) maturity as the Department has addressed its identified knowledge, skills, and abilities gaps through training or talent acquisition.

Williams Adley determined that FISMA metric question 43 is operating at a Level 4 (Managed and Measurable) maturity as the Department monitored and analyzed qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. Additionally, the Department ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

Cause, Effect, and Recommendations

Williams Adley did not identify any issues 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 2023 Maturity Rating	FY 2022 Maturity Rating
47	Use of ISCM policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier	Level 4	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 4	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 4.00 and a maturity rating of Level 4 (Managed and Measurable).

ISCM – Supplemental Reporting Metrics

The OMB identified one supplemental reporting metric for evaluation in FY 2023, as outlined in **Table 17**:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2021 Maturity Rating
48	Roles and responsibilities of ISCM stakeholders	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 determined that FISMA metric questions 47 and 49 remain at Level 4 (Managed and Measurable). However, Williams Adley identified the following minor issues related to the inconsistent implementation of defined activities:

- The (b) (7)(e) Security Assessment Report (SAR) included in the system's Authorization to Operate (ATO) package did not demonstrate the results of the most recent assessment (Condition 5).
- The (b) (7)(e) SAR included in the system's ATO package did not demonstrate the results of the most recent assessment (Condition 6).

These conditions were considered to be low risk as the Department has performed the associated control activities but did not upload the correct documentation to its system or record, CSAM, in a timely manner.

Williams Adley identified an increase in the maturity for FISMA metric question 48 from Level 3 to Level 4 (Managed and Measurable) as ISCM stakeholders are performing their respective roles and responsibilities and are held accountable for their effectiveness.

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

Cause, Effect, and Recommendations

The root cause and effect for conditions 5 and 6 were covered within the Risk Management domain. Refer to the Identify Section of the FY 2023 Audit Results for additional details.

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 2023 Maturity Rating	FY 2022 Maturity Rating
54	Processes for incident detection and analysis	Level 3	Level 3
55	Processes for incident handling	Level 4	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 3.50 and a maturity rating of Level 4 (Managed and Measurable).

Incident Response – Supplemental Reporting Metrics

The OMB identified two supplemental reporting metrics for evaluation in FY 2023, as outlined in ***Table 19***:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2021 Maturity Rating
57	Collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities	Level 4	Level 4
58	Use of technology to support its incident response program	Level 4	Level 3

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 54 remains at a Level 3 (Consistently Implemented) maturity as the Department continues to consistently implement its processes to detect and analyze incidents. However, the Department and FSA are not compliant with the EL1 and EL2 requirements at the enterprise-level (Condition 11).

Williams Adley determined that FISMA metric question 55 is operating at a Level 4 (Managed and Measurable) maturity as the Department monitors and analyses qualitative and quantitative performance measures on the effectiveness of its incident handling policies and procedures. Additionally, the Department ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

Williams Adley determined that FISMA metric question 57 is operating at a Level 4 (Managed and Measurable) maturity as the Department is currently using Einstein 3 Accelerate to detect and proactively block cyber-attacks or prevent potential compromises.

Williams Adley determined that FISMA metric question 58 is operating at a Level 4 (Managed and Measurable) maturity as the Department evaluates the effectiveness of its incident response technologies and adjusts its configurations and toolsets, as appropriate.

Cause, Effect, and Recommendations

The root cause and effect for condition 11 was covered within the Identity and Access Management domain. Refer to the Protect Section of the FY 2023 Audit Results for additional details.

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***:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2022 Maturity Rating
61	Business impact analyses (BIA) are used to guide contingency planning efforts	Level 4	Level 4
63	Performance of information system contingency plan (ISCP) tests/exercises	Level 4	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 4.00 and a maturity rating of Level 4 (Managed and Measurable).

Contingency Planning – Supplemental Reporting Metrics

The OMB identified two (2) supplemental reporting metrics for evaluation in FY 2023, as outlined in ***Table 21***:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2021 Maturity Rating
60	Roles and responsibilities of Contingency Planning stakeholders	Level 4	Level 2
65	Planning and performance of recovery activities is consistently communicated to relevant stakeholders	Level 4	Level 4

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 determined that FISMA metric question 61 is operating at a Level 4 (Managed and Measurable) maturity as the Department's resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement system contingency planning activities. Furthermore, contingency planning stakeholders are held accountable for carrying out their roles and responsibilities effectively.

Williams Adley determined that FISMA metric question 61 is operating at a Level 4 (Managed and Measurable) maturity as the Department ensures that the results of organizational and system level BIAs are integrated with enterprise risk management processes, for consistently evaluating, recording, and monitoring the criticality and sensitivity of enterprise assets.

Williams Adley determined that FISMA metric question 63 is operating at a Level 4 (Managed and Measurable) maturity as the Department utilizes automated mechanisms to test system contingency plans.

Williams Adley determined that FISMA metric question 61 is operating at a Level 4 (Managed and Measurable) maturity as the metrics on the effectiveness of recovery activities are communicated to relevant stakeholders and the Department ensures that the data supporting the metrics are obtained accurately, consistently, and in a reproducible format.

Cause, Effect, and Recommendations

Williams Adley did not identify any issues related to the Department's contingency planning program that required the issuance of a recommendation.

Appendix A. Objectives, Scope, and Methodology

Objectives

The objective of the Fiscal Year (FY) 2023 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 2023 audit began in November 2022 and ended in July 2023. For the FY 2023 audit, the Inspector General (IG) FISMA reporting metrics required that agency Office of Inspector General (OIG) or an independent assessor to evaluate the 20 core and 20 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

- Obtaining 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 2019 through FY 2022).
- 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 2023 audit covered the period July 1, 2022, to June 30, 2023, 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 2023 audit, Williams Adley obtained and inspected a population of 165 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).

(β) (7) (ε)

- Combination of Principal Offices (e.g., OCIO, FSA); and
- Combination of non-cloud and cloud-dependent systems, including cloud service providers.

Based on the criterion above, Williams Adley identified a population of 26 systems and judgmentally selected the following six out of 26 systems to determine the design and effectiveness of the Department's information security program:

(b) (7) (e)

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, and Incident Response.

FISMA Domain	Control Activity Description	Population Size	Sample Size
Identity and Access Management	Access Provisioning for New Users	515	23
Identity and Access Management	Access Removal for Separated Employees and Contractors	504	23
Identity and Access Management	Privileged User Authorization	6260	22

Identity and Access Management	Personal Identity Verification (PIV) Exemption	1941	23
Data Protection and Privacy	Equipment Sanitization for Separated Employees and Contractors	504	23
Security Training	Required Security Training for New Users	515	23
Incident Response	Incident Resolution	38	5

Table 21 – Sample Sizes for Operating Effectiveness Testing

Use of Computer-Processed Data

For the FY 2023 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 Federal Risk and Authorization Management Program (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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

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) 2023 Federal Information Security Modernization Act of 2014 audit, Williams Adley determined that:

- The only recommendation from FY 2019 remains open.
- Eight out of nine FY 2020 prior year recommendations were closed.
- All ten FY 2021 prior year recommendations were closed.
- Eight out of ten FY 2022 prior year recommendations were closed.

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

#	Description	Status	Target Action Date
FY 2019 2.4	We recommend that the Deputy Secretary require OCIO to ensure that 51 websites are routed through a trusted internet connection or managed trusted internet protocol service.	Open	03/31/2025
FY 2020 1.4	We recommend that the Chief Information Officer 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 2020 2.2	We recommend that the Deputy Secretary and Chief Operating Officer require that OCIO and FSA migrate to Transport Layer Security 1.2 or higher as the only connection for all Department connections.	Closed	-
FY 2020 2.3	We recommend that the Chief Information Officer require the Department to enhance implementation controls to prioritize and apply the most up-to-date and timely software patches and security updates to the identified systems and information technology solutions.	Closed	-
FY 2020 2.4	We recommend that the Chief Information Officer require the Department to Establish stronger monitoring controls to enforce the management of unsupported system components and track and discontinue the use of unsupported operating systems, databases, and applications. (Incorporates a Repeat Recommendation)	Closed	-
FY 2020 2.6	We recommend that the Chief Information Officer require the Department to correct or mitigate the vulnerabilities identified during the security assessment, in accordance with the severity level of each vulnerability identified.	Closed	-
FY 2020 3.1	We recommend that the Chief Information Officer require the Department to establish oversight controls to ensure the	Closed	-

	Department's password, terminations, and deactivation policies are enforced accordingly.		
FY 2020 3.2	We recommend that the Chief Information Officer require the Department to enforce the mandate for all websites to display warning banners when user's login to Departmental resources and establish additional procedures and monitoring processes to ensure that banners include the approved warning language. (Incorporates a Repeat Recommendation)	Closed	-
FY 2020 7.2	We recommend that the Chief Information Officer require the Department to develop and implement oversight controls to ensure that incidents are consistently submitted to US-CERT and the OIG within the required timeframes, are consistently categorized, and include the correct vector elements as required.	Closed	-
FY 2020 7.4	We recommend that the Chief Information Officer require the Department to develop and implement testing procedures and enhance current policies and processes to ensure that the DLP solution works as intended for the blocking of sensitive information transmission. (Incorporates a Repeat Recommendation)	Closed	-
FY 2021 3.1	We recommend that the Chief Information Officer require OCIO to—Take steps to assure obsolete solutions and encryption protocols are either updated, removed, or replaced.	Closed	-
FY 2021 3.2	We recommend that the Chief Information Officer require OCIO to—Implement additional measures for patches to be applied in a timely manner based on a priority basis.	Closed	-
FY 2021 3.3	We recommend that the Chief Information Officer require OCIO to—Ensure all Department websites are configured to mask PII when used as an identifier.	Closed	-
FY 2021 3.4	We recommend that the Chief Information Officer require OCIO to—Enforce secure connections as required by OMB M-15-13 for all existing websites and services.	Closed	-
FY 2021 4.1	We recommend that the Chief Information Officer require OCIO to—Fully implement ICAM Strategy by established milestones to ensure the Department meets full Federal government implementation of ICAM.	Closed	-
FY 2021 4.4	We recommend that the Chief Information Officer require OCIO to—Enforce a two-factor authentication configuration for all user connections to systems and applications.	Closed	-
FY 2021 4.5	We recommend that the Chief Information Officer require OCIO to—Perform and evidence regularly scheduled reviews of system user accounts (both privileged and nonprivileged) to recertify and maintain each Department system's validity.	Closed	-
FY 2021 4.6	We recommend that the Chief Information Officer require OCIO to—Remove terminated users' access to Department resources timely in accordance with Departmental policy.	Closed	-
FY 2021 4.7	We recommend that the Chief Information Officer require OCIO to—Identify and enforce all websites to display warning banners when users login to Departmental resources.	Closed	-
FY 2021 5.1	We recommend that the Chief Information Officer require the SAOP to—Implement monitoring and oversight controls that ensure employees and contractors are adhering to current media sanitization policies and are correctly documenting and validating the disposal or reuse of used digital media. In	Closed	-

	addition, provide adequate evidence showing the proper documentation and validating of clear sanitizing for all digital media assigned to the sampled 10 offboarded employees or contractors. Lastly, ensure the digital media sanitization policies and processes are completed, as appropriate, to capture all requirements dictated by Federal regulations.		
FY 2022 1.1	We recommend that the Chief Information Officer require OCIO to implement additional measures for patches to be prioritized and applied within established timeframes.	Open	06/30/2023
FY 2022 1.2	We recommend that the Chief Information Officer require OCIO to establish additional oversight controls to update, remove, or replace obsolete or unsupported solutions and encryption protocols.	Closed	-
FY 2022 2.1	We recommend that the Chief Information Officer require OCIO to ensure the Contracting Officer Representative sign, complete, and maintain Position Risk Designation forms for background investigations.	Closed	-
FY 2022 2.2	We recommend that the Chief Information Officer require OCIO to review Active Directory user accounts to enforce policy compliance for password expiration and account deactivation.	Closed	-
FY 2022 2.3	We recommend that the Chief Information Officer require OCIO to remove terminated users' access to Department resources in accordance with Departmental policy.	Closed	-
FY 2022 2.4	We recommend that the Chief Information Officer require OCIO to establish and enforce a policy to maintain and track all privileged accounts in an authorized Privileged Access Management System(s).	Open	10/31/2023
FY 2022 2.5	We recommend that the Chief Information Officer require OCIO to establish and enforce a corrective action plan to monitor and remediate identified database vulnerabilities.	Closed	-
FY 2022 3.1	We recommend that the Chief Information Officer require the Senior Agency Official for Privacy to implement monitoring and oversight controls to ensure media sanitization policies and processes are in place and document evidence of the disposal or reuse of all used digital media.	Closed	-
FY 2022 3.2	We recommend that the Chief Information Officer require the Senior Agency Official for Privacy to update digital media sanitization policies and processes to include all requirements outlined in Federal regulations.	Closed	-
FY 2022 4.1	We recommend that the Chief Information Officer require OCIO to establish oversight controls to ensure that the Department follows United States Computer Emergency Readiness Team required notification guidelines, timeframes, and communicates the relevant incidents to the OIG.	Closed	-

Appendix C. Responses to 2023 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 objective of the FY 2023 FISMA audit was to determine the effectiveness of the Department's information security program and practices as they relate to Federal information security requirements. To determine the effectiveness of the Department's information security program, Williams Adley used a risk-based approach in determining its in-scope systems. Williams Adley obtained a copy of the Department's information system inventory and applied the following criterion: • FISMA reportable system. • Federal Information Processing Standards (FIPS) 199 Categorization of "Moderate". • High-Value Assets (HVAs). • Systems containing Personally Identifiable Information (PII) or other sensitive information. (b) (7) (e) Williams Adley determined that 26 systems met at least one of the criteria above and judgmentally selected six systems (23%) to evaluate the design, implementation, and effectiveness of relevant control activities supporting the five security functions and the nine associated domains. Based on the results of the FY 2023 audit, Williams Adley determined that the Department has an effective information security program. Specifically, Williams Adley found that eight out of nine FISMA domains and the related control activities were effective in meeting the requirements established in the core and supplemental metrics. The only security domain to not reach an effective level of maturity was Identity and Access Management as issues were identified related to controls supporting the provisioning of privileged access to the selected in-scope systems and the continued use of single factor authentication for users assigned a Personal Identity Verification (PIV) exception. Additional low risk findings were found in other security domains but were considered low risk due to the Department's compensating controls or compensating circumstances. Williams Adley will issue recommendations to the Department's management team to assist them in meeting the Level 4 requirements for the Identity and Access Management domain and addressing any identified root causes.

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
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
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
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?*
	Managed and Measurable
7	*To what extent have the roles and responsibilities of internal and external stakeholders involved in cybersecurity risk management processes been defined, communicated, implemented, and appropriately resourced across the organization?*
	Managed and Measurable
8	*To what extent has the organization ensured that plans of action and milestones (POA&Ms) are used for effectively mitigating security weaknesses?*
	Managed and Measurable
9	*To what extent does the organization ensure that information about cybersecurity risks is communicated in a timely and effective manner to appropriate internal and external stakeholders?*
	Optimized
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?*
	Managed and Measurable
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 Department's risk management program is **effective**.

FISMA Question	**Supply Chain Risk Management**
12	*To what extent does the organization use an organization wide SCRM strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services?*
	Managed and Measurable
13	*To what extent does the organization use SCRM policies and procedures to manage SCRM activities at all organizational tiers?*

	Managed and Measurable
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?*
	Managed and Measurable
16.1	*Please provide the assessed maturity level for the agency's Identify - Supply Chain Risk Management program.*
	Managed and Measurable
16.2	*Please provide the assessed maturity level for the agency's Identify Function.*
	Managed and Measurable
16.3	*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 Department's supply chain risk management program is **effective**.

FISMA Question	Configuration Management
19	*To what extent does the organization use baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting?*
	Managed and Measurable
20	*To what extent does the organization use configuration settings/common secure configurations for its information systems?*
	Managed and Measurable
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?*
	Managed and Measurable
22	*To what extent has the organization adopted the Trusted Internet Connection (TIC) 3.0 program to assist in protecting its network?*
	Consistently Implemented The Department has made improvements to its configuration management program to meet the TIC requirements outlined within Office of Management and Budget (OMB) Memorandum (M) 19-26 since FY 2021, when the FISMA metric 22 was last evaluated. Specifically, the Department funded and started the migration its users from its legacy virtual private network (VPN) to a secure access service edge (SASE) architecture and created automated playbooks within its Security Orchestration Automation & Response (SOAR) solution to improve the efficiency of its security operations. Based on the most recent Technology Modernization Fund update in May 2023, the Department expects to migrate approximately 35% of its systems behind SASE by the second half of calendar year 2023. Additionally, the Department is in process of improving its maturity across all Zero Trust Pillars. Additionally, Williams Adley determined that the Department is making significant progress to remediate the FY 2019 open recommendation 2.4 related to ensuring that websites are routed through a trusted internet connection. As of the conclusion of the FY 2023 FISMA

	audit, the Department only has [redacted] TIC non-compliant websites remaining from the 51 identified in FY 2019. Once remediated and resolved, the Department will be able to fully monitor and review the implemented TIC 3.0 use cases to determine effectiveness and incorporates new/different use cases, as appropriate. Williams Adley neither identified any conditions nor issued any recommendations for metric 22 as the Department is working through its plan to meet compliance with M-19-26.
24	*To what extent does the organization use a vulnerability disclosure policy (VDP) as part of its vulnerability management program for internet accessible federal systems?*
	Managed and Measurable
25.1	*Please provide the assessed maturity level for the agency's Protect - Configuration Management program.*
	Managed and Measurable
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 Department's configuration management program is **effective**.

FISMA Question	Identity and Access Management
26	*To what extent have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?*
	Consistently Implemented Williams Adley determined that ICAM stakeholders are mostly performing their identity and access management roles and responsibilities. However, the issues identified in FISMA metric questions 27, 30, and 32 indicate that the IAM activities are not performed effectively and designed.
27	*To what extent does the organization use a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities?*
	Consistently Implemented Williams Adley determined that the Department is making progress towards accomplishing the milestones outlined within its ICAM strategy and technology solution road map. At the conclusion of the FY 2023 audit period, Williams Adley determined that the Department had not completely integrated the following elements: bidirectional synchronization of the active directory, credential management, and single sign on. Single sign-on was completed at [redacted] Additionally, the Department has not started the decommission of the [redacted] (b) (7) (e) Despite the Department not fully implementing its ICAM strategy, it has introduced elements of Level 4 maturity within its environment, including the use of automation to manage and review user access agreement for privileged and non-privileged users. Williams Adley neither identified any conditions nor issued any recommendations for metric 27 as the Department is working through the milestones outlined within its ICAM strategy and roadmap.

29	*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
30	*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 not discontinued the use of its PIV exemption process which allows non-privileged users to authenticate against the network using single factor authentication. For system level access, the Department has implemented multifactor authentication.
31	*To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO2, or web authentication) for privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?*
	Managed and Measurable
32	*To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed?*
	Defined Williams Adley determined that the Department has defined its processes for provisioning, managing, and reviewing privileged accounts. However, the Department did not consistently implement its defined controls activities to ensure that privileged end user access is appropriately requested and approved. Specifically, Williams Adley found the following issues related to the implementation of its access provisioning controls for two in-scope systems: • Five sampled users granted privileged access during the audit period did not complete an elevated access request form. • One sampled user granted privileged access during the audit period did not complete any onboarding forms, including an elevated access request form. Additionally, the Department did not implement identity and credential management logging requirements for privileged users required for EL2 maturity, in accordance with M-21-31.
33	*To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions?*
	Managed and Measurable
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 Department's identity and access management program is **not effective**.

FISMA Question	Data Protection and Privacy
35	*To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems?*
	Managed and Measurable
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
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 Department's data protection and privacy program is **effective**.

FISMA Question	Security Training
41	*To what extent have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?*
	Managed and Measurable
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?*
	Managed and Measurable
43	*To what extent does the organization use a security awareness and training strategy/plan that leverages its skills assessment and is adapted to its mission and risk environment?*
	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 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?*
	Managed and Measurable
48	*To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization?*
	Managed and Measurable
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?*
	Managed and Measurable
51.1	*Please provide the assessed maturity level for the agency's Detect - ISCM function.*
	Managed and Measurable
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 Department's ISCM program is **effective**.

FISMA Question	Incident Response
54	*How mature are the organization's processes for incident detection and analysis?*
	Consistently Implemented: Williams Adley determined that the Department has consistently implemented its policies, procedures, and processes for incident detection and analysis. However, the Department and FSA are not compliant with the EL1 and EL2 requirements at the enterprise-level. Furthermore, the Department has not implemented profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents.
55	*How mature are the organization's processes for incident handling?*
	Managed and Measurable
57	*To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support?*
	Managed and Measurable
58	*To what extent does the organization use the following technology to support its incident response program?*
	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 Department's incident response program is **effective**.

FISMA Question	Contingency Planning
60	*To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined, communicated, and implemented across the organization, including appropriate delegations of authority?*
	Managed and Measurable
61	*To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts?*
	Managed and Measurable
63	*To what extent does the organization perform tests/exercises of its information system contingency planning processes?*
	Managed and Measurable
65	*To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk-based decisions?*
	Managed and Measurable
66.1	*Please provide the assessed maturity level for the agency's Recover - Contingency Planning function.*
	Managed and Measurable
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 Department's contingency planning program is **effective**.

Appendix D. Department of Education Management Response

UNITED STATES DEPARTMENT OF EDUCATION

DATE: August 30, 2023

TO: Kevin J. Young
Assistant Inspector General
Information Technology Audits and Computer Crime Investigations Office of Inspector General

FROM: Luis Lopez
Chief Information Officer

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 2023
Control Number A23IT0118

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 2023*, Control Number A23IT0118. 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. We appreciate OIG's exceptional efforts to provide strategic and meaningful recommendations while balancing substantial changes in methodology and timelines this year. We also appreciate the recognition of the Departments commitment, and our ongoing progress, to strengthen the overall cybersecurity of its networks, systems, and data, as reflected in the draft report.

Risk Management

The Department's accomplishments in maturing its risk management capabilities, specifically the maturation of the Cybersecurity Framework (CSF) Risk Scorecard, has been recognized by other Federal Agencies, including OMB, as an optimized capability in managing and communicating cybersecurity risk. The Department of Commerce (DOC), Department of Justice (DOJ), Department of Transportation (DOT), 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) 2023, the Department has continued its maintenance, enhancement, and capability of its CSF Risk Scorecard (v3.0), released November 7, 2022. Version 3.0 of the ED CSF Risk Scorecard integrates the alignment of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 5 security and privacy controls to the NIST CSF Version (Ver.) 1.1

and the NIST Privacy Framework (PF) Ver. 1.0.

The ED CSF Risk Scorecard provides continuous measurement and risk prioritization of key metrics for system stakeholders, Principal Office Component (POC) leadership, and Department executive leadership on a daily, monthly, and quarterly basis. Providing prioritization for risk mitigation at an information system boundary based on identified user defined criticality of risk levels and enterprise prioritization through the appropriate information system weighting, to include high value asset (HVA) characterizations, which we just obtained full certification for self-assessments, within the Department. The ED CSF Risk Scorecard also has a daily Data Discrepancy Report (DDR) component that performs continuous validation of the information maintained within the Department governance, risk, and compliance (GRC) tool, Cyber Security Assessment and Management (CSAM), which is developed by the Department of Justice (DOJ).

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 2022 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 OSA program in accordance with roles and responsibilities established within the Information Technology (IT) System Security Assessment and Authorization (CA) Standard. ED has enrolled 102 FISMA reportable systems, 28 Cloud Service Providers (CSP), and 8 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 CSAM 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.

On February 27, 2023, OMB Memorandum M-23-13, *"No TikTok on Government Devices" Implementation Guide*, was issued. ED issued the appropriate CISO memorandum to all ED employees and contractors to remove TikTok and any successor application or service developed or provided by ByteDance Limited or subsidiary from ED devices and providing instructions and deadlines for its removal.

Supply Chain Risk Management

The integration of supply chain risk management (SCRM) assessments with the ED Enterprise Architecture Technology Insertion process, also known as the EA (TI) process, successfully identified 15 CFR Part 7 concerns with (b) (7) (e) resulting in Deep Dive reviews and the creation of plan of action and milestones (POA&Ms) for mitigation. SCRM has also been integrated into the CSF Risk Scorecard to strengthen the ability to measure and monitor supply chain risk.

Over the course of FY 2023, the Information and Communications Technology (ICT) SCRM methodology has continued to mature and align with NIST SP 800-161, Rev. 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, and recommendations provided from the U.S. Government Accountability Office (GAO). ED evaluates and measures SCRM risk at each of the three-tiers of the organization: Enterprise (Tier 1 – strategic), POC (Tier 2 – operational), and Information System (Tier 3 – tactical). ED released the *Department Information Security and Privacy Requirements* (Version 2.3 published May 4, 2023) setting forth the security and privacy requirements of the Department, and *Information Technology (IT) System Supply Chain Risk Management (SR) Standard* (Version 1.3 published

March 10, 2023) setting forth updated SCRM standards and expectations to be integrated throughout the Department. With the release of the ED CSF Risk Scorecard v3.0, the NIST SP 800-53, Rev. 5 SR security and privacy controls were officially integrated into the scoring metrics for all information systems in preparation for the ED information systems' transition from NIST SP 800-53, Rev. 4 to NIST SP 800-53, Rev. 5.

The SCRM program has also integrated with the ED Enterprise Architecture Technology Insertion process, also known as the EA (TI) process, allowing the SCRM team to review software and hardware during the initiation and requirement phases of the system lifecycle (SLC). This integration has permitted ED to identify risks and permitted senior leadership the appropriate capability of accepting, mitigating, or transferring of risk within the Department.

The SCRM evaluation identified [redacted] (b) (7) (e) 15 CFR Part 7 manufacturing concerns during the EA (TI) assessment triggering an SCRM Deep Dive Assessment resulting in the creation of a POA&M to address and remove the affected systems from ED networks. Also concerns were identified [redacted] (b) (7) (e) which resulted in Deep Dive Assessments and POA&Ms for removal. [redacted] (b) (7) (e), while developed primarily in [redacted] (b) (7) (e) has [redacted] (b) (7) (e) as a major financial supporter and the Chief Technology Officer (CTO) of [redacted] (b) (7) (e) is on the Board of Directors. [redacted] (b) (7) (e) is developed and maintained in the Russian Federation and has added concerns relating to the ongoing hostilities with Ukraine.

ED has also become a member of the Government-Industry Data Exchange Program (GIDEP), providing supply chain risk intelligence resource and information sharing capacities of the organization and among other government and industry participants.

Configuration Management

The Department was the first cabinet-level Department to receive funding from the Technology Modernization Fund (TMF) and successfully adopted a secure access service edge (SASE) solution in support of advancing its Zero Trust Architecture (ZTA) capabilities in support of federal requirements as outlined in OMB Memorandum M-22-09.

The Department issued a contract on September 22, 2022 for the establishment of a ZTA Project Management Office (PMO), modified an existing enterprise contract on September 28, 2022 for the procurement of SASE and security orchestration, automation, and response (SOAR) capabilities, and selected a professional service provider to modernize and enhance its enterprise identify, credential, and access management (ICAM) solution on September 1,2022. These actions have been possible through the utilization of the funding from the TMF.

The Department was able to leverage its newly deployed zero trust architecture (ZTA) tools, secure access service edge (SASE), to begin blocking TikTok by its application identifier. In the month of April 2023 ED blocked 65,000 access attempts by approximately 2,800 users, and May 2023 ED blocked 150,000 access attempts by approximately 3,700 users, accounting for a 100% successful block rate to the service.

ED is also leveraging the ZTA SASE solution to deploy the trusted internet connections (TIC) 3.0 capabilities enterprise wide. ED has also acquired enhanced managed trusted internet protocol service (MTIPS) through the General Services Administration (GSA) Enterprise infrastructure Solutions (EIS).

Identity and Access Management

The ED enterprise identity, credential, and access management (ICAM) program was successful in integrating with Login.gov for public users and was integral to instituting multifactor authentication (MFA) deployment across the Department through integrating personal identity verification (PIV) validation of ED organizational users. As a result, the Department improved the MFA compliance of its system inventory from (b) (7)(e) deployment at end of FY 2023 Quarter 1 to (b) (7 (e) deployment at end of FY 2023 Quarter 2. From a data encryption perspective, as of FY 2023 Quarter 3, the Department has achieved (b) (7) (e) data at rest (DAR) implementation compliance and (b) (7 (e) data in transit (DIT) compliance.

The Department issued a contract with a professional service provider to modernize and enhance its Enterprise ICAM solution beginning September 1, 2022 and align with the OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* requirements to meet specific cybersecurity standards and objectives by the end of FY 2024. The ICAM program continues to provide improved security features and functionality which enhance the security posture of the Department. The Enterprise ICAM service has been working to integrate all 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 their Microsoft Office 365 applications.

Enterprise ICAM provides the following new capabilities to ED: 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 that align with OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, and OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, for user and privileged user logging requirements.

Enterprise ICAM has integrated Login.gov authentication services for external users (i.e., public) to leverage a single secure sign-in authenticator to ED applications through an interagency agreement (IAA) with U.S. General Services Administration (GSA). This capability will permit ED information systems to leverage this single secure sign-in authenticator for public users, be able to correlate log data across information systems throughout the Enterprise to gain insight to user account-based attacks, and streamline our public user authentications into services provided by ED.

FSA has instituted a solution, (b) (7 (e) and (b) (7 (e) (b) (7 (e) allowing 21 million students to utilize MFA to protect their accounts and reduce the opportunity for potential fraud associated with compromised identities, and has enhanced its capability of leveraging enhanced identity verification capabilities using third-party services (e.g., TransUnion). FSA has also further implemented risk-based authentication (RBA) solutions leveraging Federal Risk and Authorization Management Program (FedRAMP) approved tools and web application firewalls (WAF).

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 an: ED privacy program to ensure compliance with all applicable statutes, regulations, and policies regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of personally identifiable information (PII) by POCs and information systems; privacy policy; and evaluating and managing privacy risks at the Department.

The Department has reviewed and updated the four (4) core Departmental Directives (ACSD) that establish policy governing privacy: ACSD-OPEPD-002, *Personally Identifiable Information Breach Response Policy and Plan* published 11 APR 2023; ACSD-OPEPD-004, *Privacy Act of 1974 (The Collection, Use, and Protection of Personally Identifiable Information)* published 26 APR 2023; ACSD-OPEPD-003, *Privacy: Section 208 of the E-Government Act of 2002 Policy and Compliance* published 27 FEB 2023; and ACSD-OCIO-004, *Cybersecurity Policy* published January 12, 2023. Integrated privacy guidance into the twenty (20) Department information security and privacy standards aligned to each NIST SP 800-53, Rev. 5 security and privacy control family.

The Privacy Program has also integrated with the OCIO Information Assurance Services (IAS) Risk Assessment Services (RAS) program OSA process. This integration ensures that the privacy components are managed on an ongoing basis. The OSA processes evaluate all systems, onboarded into OSA, to ensure their privacy threshold analysis (PTA), privacy impact assessment (PIA), system of records notice (SORN), quantity of PII, and privacy system classification are accurately maintained and reported within the ED GRC tool. Any weaknesses identified result in POA&Ms being created against the appropriate information system boundary to accurately track the identified discrepancy through to compliance. Any discrepancies as well as any upcoming document compliance expirations are captured on and reported on a quarterly basis within the OSA Quarterly Report to the Security Assessment Team (SAT) Contracting Officer's Representative (COR), ED Chief Information Security Officer (CISO), SAOP, and ED CIO.

With the release of the ED CSF Risk Scorecard v3.0, the NIST SP 800-53, Rev. 5 privacy control baseline was officially integrated into the scoring metrics for all information systems in preparation for the ED information systems' transition from NIST SP 800-53, Rev. 4 to NIST SP 800-53, Rev. 5. Further a privacy score is now calculated and factored into the ED CSF Risk Scorecard based on the NIST PF Ver. 1.0. By integrating the NIST CSF and the NIST PF into the ED CSF Risk Scorecard v3.0, ED leadership, to include the SAOP and CIO, gain a holistic view of the risks within the Department. Further the scorecard provides the capability to continuously monitoring – daily, monthly, and quarterly – of the status of the key privacy documents (e.g., PTA, PIA, SORN) and metrics (e.g., documentation approved within appropriate timelines, quantity of PII within an information system, PII classification of an information system).

Security Training

The Department continued to build on FY 2022 awards and received multiple recognitions and awards in FY 2023 from the Federal Information Security Educators Association (FISSEA). FISSEA is an organization run by and for Federal government information security professionals to assist Federal agencies in strengthening their employee cybersecurity awareness and training programs. Following receipt of these awards, the Department of Energy (DOE), Postal Regulatory Commission (PRC), Social Security Administration (SSA), Department of Health and Human Services (HHS), Department of Labor (DOL), Department of Commerce (DOC), and Consumer Financial Protection Board (CFPB) reached out to the Department and requested meetings to learn more about the Department's program and obtain guidance and direction on how to build and maintain an effective training program.

The ED security training program hosted the FY 2023 Cybersecurity Symposium each Thursday throughout October 2023. Over 1,000 employees and contractors attended over the four weeks, serving as the largest attendance to date.

In November 2022, the Department received recognition and multiple awards from the FISSEA. FISSEA is an organization run by and for Federal government information security professionals to assist Federal agencies in strengthening their employee cybersecurity awareness and training programs. These awards include Awareness Training Category award for the Cybersecurity and Privacy Awareness (CSPA1) Escape Room course; Innovative Solutions award for badges awarded for high levels of symposium participation and top reporters of phishing exercises; and Awareness Newsletter award for the Department's Bits and Bytes awareness newsletter.

Following receipt of these awards, the Department of Energy (DOE), Postal Regulatory Commission (PRC), Social Security Administration (SSA), Department of Health and Human Services (HHS), Department of Labor (DOL), Department of Commerce (DOC), and Consumer Financial Protection Board (CFPB) reached out to the Department and requested meetings to learn more about the Department's program and obtain guidance and direction on how to build and maintain an effective training program. 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.

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 2022 and identified actions required to achieve plan goals in FY 2023. The FY 2022 to FY 2023 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. Updates to the FY 2022 Cybersecurity Awareness and Training Program Summary Report document actions taken to maintain and strengthen the program and updates to the Simulated Phishing Exercise Plan enabled the Department to identify trends from FY 2022 exercises and plan for FY 2023 exercises. This plan is used to guide exercise conduct, increase resiliency, reduce susceptibility, and reduce behavioral risk to the Department. Program standard operating procedures (SOP) were updated to enhance the program through new or modified processes.

On November 18, 2022, ED released FY 2023 Requirements for Role-Based Training for Personnel with Significant Security Responsibilities (SSR). The purpose of this memo was to ensure personnel with SSR received specific skills training and education required to develop and maintain a cybersecurity workforce capable of actively reducing and managing risk to ED information and information systems.

The Department launched and executed three (3) Cybersecurity and Privacy Awareness (CSPA) training courses in FY 2023 providing continual user awareness training; enabling users to define cyber risk management; educate 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.

ED has executed five (5) simulated phishing exercises in FY 2023. These exercises reflect 98.5% of users assessed successfully passed the exercise by properly identifying the email communication as phishing and in the first four of these exercises an average of 55.7% of users reported the phishing email to the appropriate individuals. On March 8, 2023, ED saw the benefits of this training through an employee appropriately reporting a potential phishing email to the ED Security Operations Center (EDSOC), which was confirmed to be a legitimate attack against an employee. Due to the message being appropriately reported and investigated, the employee protected the Department and a fellow employee against the phishing scam attack.

ED replaced phishing exercise result email notifications and spreadsheets with an automated phishing dashboard. This tool provides 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*, published February 28, 2023, requirements. This dashboard is used by OCIO IAS and is made available to POC Executive Officers, assistant secretaries, and senior leadership to provide full visibility of user performance in Department-led phishing exercises.

ED also continued publishing the training dashboard; this dashboard visualizes compliance with mandatory training and strengthens the ability of information system security officers (ISSO) 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. The dashboard enables the Department to track training metrics by course, POC, user status (employee or contractor), and fiscal year.

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 5.01 published November 15, 2022). 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 team focuses on ensuring the quality of data within the necessary reporting tools to include CSAM, EDCDL, SCRM, and CDM. The Department understands that continuous monitoring activities is only as good as the data it is managing. 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 remediated; 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 have been no major cybersecurity incidents across the Department in FY 2023. To bolster collaboration and inter-agency coordination, ED has also allocated a dedicated resource to work with law enforcement (LE) and the National Cyber Investigative Joint Task Force (NCIJTF). 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 enterprise security information and event management (SIEM) solution, EDCDL, 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.

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.

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.

Currently, the Department has configured all operating systems, including Linux and Windows, data input for ingestion into the EDCDL. The Department is now tracking a combined ED and FSA enterprise logging environment and are nearing [redacted] EL1 compliance, as defined in OMB Memorandum M-21-31, with a slight day-to-day various. However, as described within the ISCM program, there are numerous dashboards tracking compliance providing the Department the ability to troubleshoot any reporting deviations for compliance mitigation. Through this enterprise log aggregation within the EDCDL, enterprise security risk alerting has been deployed based on the correlation of log data to include the capabilities for expanding and understanding searches, threat intelligence, and asset identities.

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. However, establishing a dedicated line of funding for enterprise IT and cybersecurity programs would allow the Department the means to adequately fund EO 14028 initiatives, and ensure an adequate recruitment, retention, and incentive pay flexibilities to fully address its cybersecurity gaps and compete with the Federal enterprise and private sector cyber workforce.

1.1: Williams Adley recommends that Chief Information Officer requires the Department and FSA to take immediate corrective actions to implement enhanced monitoring procedures to allow for timely review of system authorization packages and appropriate authorization prior to submission into CSAM.

Management's Response: The Department concurs with this recommendation and will continue this effort in FY 2024 and develop a corrective action plan by October 31, 2023.

3.1: Williams Adley recommends that Chief Information Officer requires the Department to develop and implement an effective quality control review process for its policies and procedures.

Management's Response: The Department concurs with this recommendation and will continue this effort in FY 2024 and develop a corrective action plan by October 31, 2023.

4.1: Williams Adley recommends that Chief Information Officer requires the Department and FSA to take immediate corrective actions to remove users from PIV exempt list.

Management's Response: The Department concurs with this recommendation and proactively completed remediation in April 2023.

4.2: Williams Adley recommends that Chief Information Officer requires 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.

Management's Response: The Department concurs with this recommendation and will continue this effort in FY 2024 and develop a corrective action plan by October 31, 2023.

4.3: Williams Adley recommends that the Chief Information Officer require that the Department and 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.

Management's Response: The Department concurs with this recommendation and will continue this effort in FY 2024 and develop a corrective action plan by October 31, 2023.

5.1: Williams Adley recommends that Chief Information Officer requires the Department to update Department PIA processes, quality control procedures, and monitoring controls to validate, track, and enforce the timely completion and review of PIAs.

Management's Response: The Department concurs with this recommendation and will continue this effort in FY 2024 and develop a corrective action plan by October 31, 2023.

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

Appendix E. FY 2023 Conditions, Associated Criteria, and Recommendation Issued[10]

#	FISMA Metric Domain	Condition Description	Associated Criteria	Recommendation Issued
1	Risk Management	The Department of Education (Department) did not consistently identify standard data elements/taxonomy for managing hardware inventory for its systems. Specifically, [redacted] (b) (7 (e)	The Configuration Management Standard, dated February 9, 2023, control CM-8 System Component Inventory states: • 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 tracking and reporting; and ○ Includes the following information to achieve system component accountability: as defined in Cyber Security Assessment and Management System (CSAM) System Information, Appendix S Hardware Listing and System Information, Appendix T Software Listing; not required for [Cloud Service Provider (CSP)] or Shared Services. • Review and update the system component inventory at a minimum quarterly.	This condition was deemed low risk as both systems are managed by external parties and subject to the Department's supply chain risk management processes. As a result, Williams Adley will not issue a recommendation to address this condition.
2	Risk Management	The Department did not consistently identify standard data elements/taxonomy for managing software inventory for its systems. Specifically, the following in-scope systems' software inventory did not capture the required "serial/license number" and "install/effective date" values for the software components: [redacted] (b) (7 (e)		This condition has minimal impact on the Department's maturity as the Department has already identified the issue and created a plan of action and milestone to address the root cause. As a result, Williams Adley will not issue a recommendation to address this condition.

[10] All recommendations issued for the FY 2023 reporting period remain open as of the date of this report.

		- (b) (7 (e)		
3	Risk Management and Information Security Continuous Monitoring	(b) (7 (e) System Security Plan (SSP) Review Checklist was not signed by the Information System Owner (ISO) and Information System Security Officer (ISSO).	According to the Information Technology (IT) System Planning Standard dated December 5, 2022, SSP Review Checklist requires signatures from the ISO and ISSO and updated on an annual basis. The SSP Standard Operating Procedures (SOP) dated October 12, 2022, states that SSP review, and acceptance process is a formal process which references security requirements for an information system and ensures security controls are in place or planned for meeting those requirements as outlined in the National Institute of Standard and Technology (NIST) Special publication (SP) 800-18. The IT System Security Assessment and Authorization (CA) Standard dated January 31, 2023, requires assessing the controls in the system and its environment of operation at least annually using independent assessors, self-assessments, or ongoing security control monitoring/ongoing security authorization processes to determine the extent to which the controls are implemented.	Recommendation 1.1: Williams Adley recommends that Chief Information Officer requires the Department and FSA to: Take immediate corrective actions to implement enhanced monitoring procedures to allow for timely review of system authorization packages and appropriate authorization prior to submission into CSAM.
4	Risk Management and Information Security Continuous Monitoring	The (b) (7 (e) SSP Review Checklist was not performed annually, last updated February 11, 2021.		
5	Risk Management and Information Security Continuous Monitoring	The FMS Security Assessment Report (SAR) included in the system's Authorization to Operate (ATO) package did not demonstrate the results of the most recent assessment.		
6	Risk Management and Information Security Continuous Monitoring	The (b) (7 (e) SAR included in the system's ATO package did not demonstrate the results of the most recent assessment.		
7	Configuration Management	The Software Management and Acquisition Policy, last updated on April 10, 2019, requires annual revision.	The Software Asset Management and Acquisition Policy dated April 10, 2019, states that this policy document is reviewed annually. The due date is determined by the final approved and signed date by the Assistant Secretary, Office of Finance and Operations or by his/her duly designated representative.	Recommendation 3.1: Williams Adley recommends that Chief Information Officer requires the Department to develop and implement an effective quality control review process for its policies and procedures.
8	Configuration Management	The following in-scope systems refer to the rescinded/retired Baseline Standard within the control implementation statement for	According to the System Planning Standard dated December 5, 2022, control PL-2 System Security and Privacy Plans states: • Distribute copies of the plans and communicate subsequent changes to the plans	Recommendation 1.1: Williams Adley recommends that Chief Information Officer requires the Department and FSA to take immediate corrective actions to implement enhanced

		minimum security controls in their respective SSP and CSAM tool: (b) (7 (e)	to personnel with cybersecurity and privacy responsibilities, including but not limited to the Authorizing Official (AO) or AO delegate, ISSO, and ISO. • Review the plans at least annually or when a major change occurs to the system. • Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments. • Protect the plans from unauthorized disclosure and modification	monitoring procedures to allow for timely review of system authorization packages and appropriate authorization prior to submission into CSAM.
9	Identity and Access Management	The Department and Federal Student Aid (FSA) did not (b) (7 (e)	The Memorandum Recission of Department Standard PR.AC: Emergency PIV Alternative, dated April 22, 2022, requires that: • Effective sixty days from the issuance of this memorandum, Standard PR.AC: Emergency PIV Alternative Standard is rescinded, and as required by Homeland Security Presidential Directive 12 (HSPD-12): “Policy for a Common Identification Standard for Federal Employees and Contractors,” all federal employees and contractors are required to use a Personal PIV smartcard (badge) for authentication and access to Federal facilities and IT systems. • During this timeframe, Office of the Chief Information Officer (OCIO) will be 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	Recommendation 4.1: Williams Adley recommends that Chief Information Officer requires the Department and FSA to take immediate corrective actions to remove users from PIV exempt list.

			sixty days, OCIO will stop deploying laptops with PIV-Alternate configuration.	
10	Identity and Access Management	The Department and FSA did not properly grant access to its users. Specifically, • All three sampled [redacted] users did not complete elevated access request form. • Two out of three sampled [redacted] users did not complete elevated access request form. • One out of three sampled [redacted] user did not complete any onboarding forms, including an elevated access request form. • All eight sampled [redacted] users did not complete any onboarding forms, including an elevated access request form.	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision (Rev) 5, "Security and Privacy Controls for Information Systems and Organizations": AC-2 Account Management Control: • Define and document the types of accounts allowed and specifically prohibited for use within the system. • Assign account managers. • Require [Assignment: organization-defined prerequisites and criteria] for group and role membership. • Specify: o Authorized users of the system. o Group and role membership; and o Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account. • Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts. • Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]. • Monitor the use of accounts. • Notify account managers and [Assignment: organization-defined personnel or roles] within: o [Assignment: organization-defined time period] when accounts are no longer required. o [Assignment: organization-defined time period] when users are terminated or transferred; and	Recommendation 4.2: Williams Adley recommends that Chief Information Officer requires 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.

			o [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual. • Authorize access to the system based on: o A valid access authorization. o Intended system usage; and o [Assignment: organization-defined attributes (as required)]. • Review accounts for compliance with account management requirements [Assignment: organization-defined frequency]. • Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and • Align account management processes with personnel termination and transfer processes. The Information Technology (IT) System Access Control (AC) Standard, dated February 10, 2023, in the Control Overlay AC-2 ED-01 (L, M, H), requires the Department to uniquely identify and authenticate each service attempting to access EO-critical software or EO-critical software platforms.	
11	Identity and Access Management and Incident Response	The Department of Education (Department) and Federal Student Aid (FSA) are not compliant with EL1 and EL2 requirements at the enterprise-level.	The Office of Management and Budget (OMB) Memorandum (M)-21-31, “Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents,” establishes requirements for agencies to increase the sharing of such information, as needed and appropriate, to accelerate incident response efforts and to enable more effective defense of Federal information and executive branch departments and agencies. This memo establishes a maturity model to guide the implementation of requirements across four EL tiers, as described below:	Recommendation 4.3: Williams Adley recommends that the Chief Information Officer require that the Department and 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.

			• EL0 Not Effective Logging requirements of highest criticality are either not met or are only partially met. • EL1 Basic Only logging requirements of highest criticality are met. • EL2 Intermediate Logging requirements of highest and intermediate criticality are met. • EL3 Advanced Logging requirements at all criticality levels are met. Furthermore, Agencies must immediately begin efforts to increase performance in accordance with the requirements of this memorandum. Specifically, agencies must: • Within 60 calendar days of the date[11] of this memorandum, assess their maturity against the maturity model in this memorandum and identify resourcing and implementation gaps associated with completing each of the requirements listed below. Agencies will provide their plans and estimates to their OMB Resource Management Office (RMO) and Office of the Federal Chief Information Officer (OFCIO) desk officer. • Within one year of the date of this memorandum, reach EL1 maturity. • Within 18 months of the date of this memorandum, achieve EL2 maturity.	
12	Data Protection and Privacy	The Department did not review and update, as applicable, the [redacted] (b) (7) (e) Privacy Impact Assessment (PIA) within a two-year cycle, as required.	The Information Technology (IT) System Planning (PL) Standard, dated December 2022, states that the PIA must be reviewed every two years and approved by the Information System Security Officer (ISSO), Information System Officer (ISO), Privacy Safeguards Division, and Senior Agency Official for Privacy (SAOP).	Recommendation 5.1: Williams Adley recommends that Chief Information Officer requires the Department to update Department PIA processes, quality control procedures, and monitoring controls to validate, track, and enforce the timely completion and review of PIAs.

[11] August 27, 2021