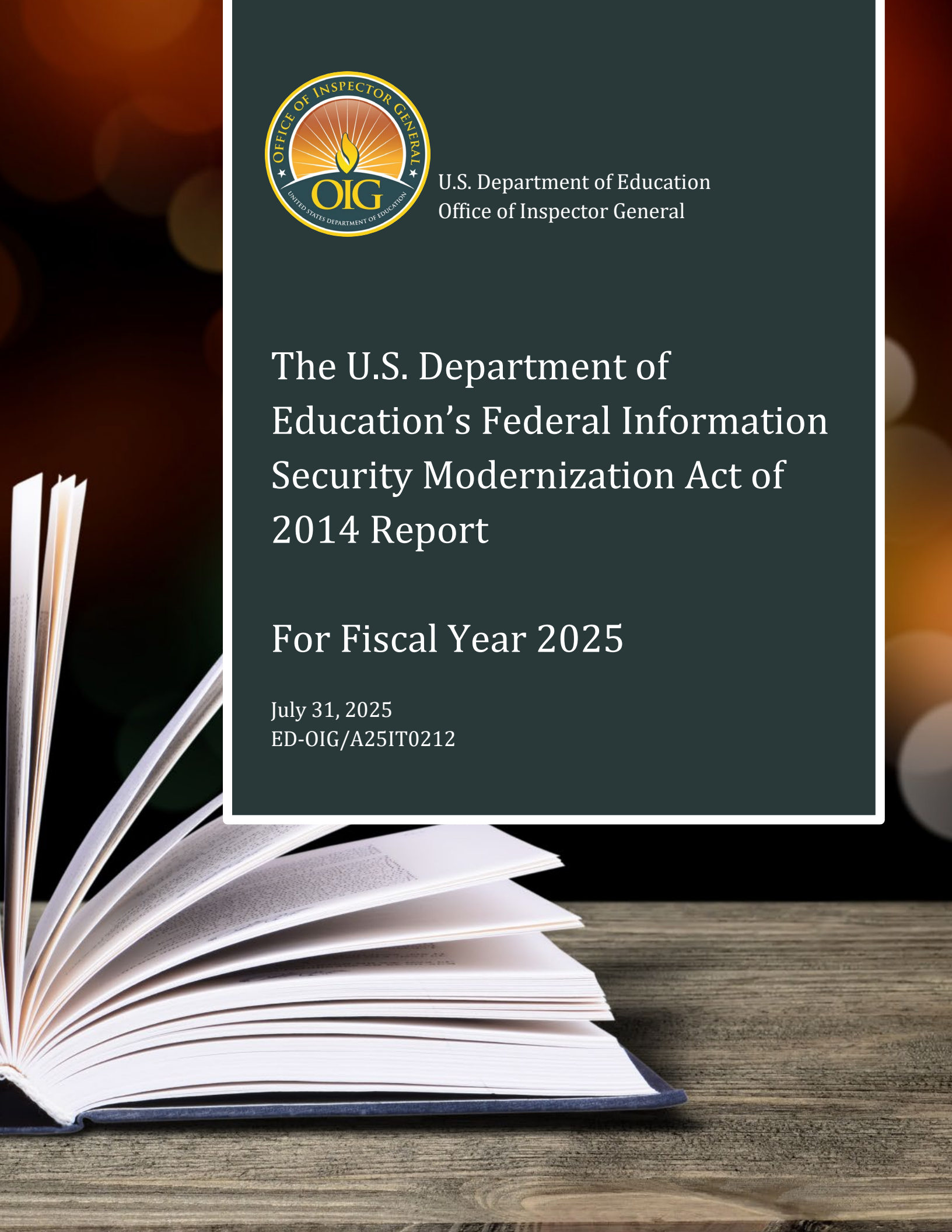

U.S. Department of Education
Office of Inspector General

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

For Fiscal Year 2025

July 31, 2025
ED-OIG/A25IT0212

July 31, 2025

TO: Thomas N. Flagg
Chief Information Officer
Office of the Chief Information Officer

FROM: Keith Cummins /s/
Acting Deputy Assistant Inspector General
Audit Services
Office of Inspector General

SUBJECT: Final Audit Report
Federal Information Security Modernization Act of 2014 Audit of the U.S. Department of Education's Information Security Program and Practices for Fiscal Year 2025
Control Number ED-OIG/A25IT0212

Attached is the **final audit report** that determined whether the U.S. Department of Education's (Department) overall information technology security programs and practices are effective as they relate to Federal information security requirements. We contracted with the independent certified public accounting firm of Williams, Adley & Company – DC, LLC (Williams Adley) to conduct this audit. The audit assessed the information and information system security controls in place during the period of July 1, 2024, to June 30, 2025.

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

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

An electronic copy has been provided to your Audit Liaison Officer. Williams Adley received and evaluated the Office of the Chief Information Officer (OCIO) management comments in response to the

findings and recommendations in the report. OCIO agreed to provide corrective action plans for all recommendations by September 30, 2025.

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 restated (5 U.S.C. §§ 401–424), the Office of Inspector General is required to report to Congress twice a year on recommendations that have not been completed after 6 months from the date of issuance.

In accordance with the Freedom of Information Act (5 U.S.C. § 552), reports issued by the Office of Inspector General 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.

We appreciate the cooperation shown to Williams Adley and the OIG during this audit. If you have any questions, please contact Joseph Maranto, Director, Information Technology Oversight Team at 202-245-7044 or joseph.maranto@ed.gov.

Attachment

cc: Richard Smith, Deputy Secretary, Delegated, Office of the Deputy Secretary
James Bergeron, Acting Under Secretary, Office of the Under Secretary and Acting Chief Operating Officer, Federal Student Aid
Ray Crawford, Acting Deputy Chief Information Officer, Office of the Chief Information Officer
Davon Tyler, Acting Chief Technology Officer, Federal Student Aid
Peter Hoang, Acting Chief Information Security Officer, Office of the Chief Information Officer
Robert Anderson, Acting Chief Information Security Officer, Federal Student Aid
Bucky Methfessel, Senior Counsel for Information & Technology, Office of the General Counsel
Ruth T. Dunlop, Audit Accountability and Resolution Tracking System Administrator, Office of Inspector General

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

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

Report for Fiscal Year 2025

July 29, 2025

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 (OIG). Any appropriate corrective actions to address the conclusions within this report will be determined by the relevant United States Department of Education stakeholders. In accordance with Freedom of Information Act (Title 5, United States Code, Section 552), reports that the OIG issues are available to members of the press and public to the extent information they contain is not subject to exemptions in the Act.

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

WILLIAMS ADLEY

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

Dear Mr. Flagg:

We are pleased to provide our report outlining the results of the performance audit conducted to determine the effectiveness of the United States Department of Education's (Department) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) for the fiscal year (FY) 2025.

On January 15, 2025, the Office of Management and Budget (OMB) issued Memorandum M-25-04 ("Memorandum for the Heads of Executive Departments and Agencies: [FY] 2025 Guidance on Federal Information Security and Privacy Management Requirements") to provide instructions for meeting the FY 2025 FISMA reporting requirements.

To achieve this objective, we reviewed the FY 2025 Inspector General FISMA reporting metrics and performance measures selected by OMB and conducted this performance audit in accordance with Generally Accepted Government Auditing Standards which requires that we obtain sufficient, appropriate evidence to provide a reasonable basis for our conditions and conclusions. We believe that the evidence obtained throughout the FY 2025 audit provides a reasonable basis for our conclusions and maturity ratings.

Based on the audit procedures performed for the FY 2025 audit period, Williams Adley concluded that the Department has met the requirements to be operating at an effective level of security, for the subset of information systems evaluated, as outlined within the FY 2025 FISMA reporting metrics. The details supporting our conclusion are found in the attached report.

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

/s/

July 29, 2025

WILLIAMS, ADLEY & COMPANY-DC, LLP
Certified Public Accountants / Management Consultants
1060 16th Street, NW, Suite 400 • Washington, DC 20036 • (202) 371-1397 • Fax: (202) 371-9161
www.williamsadley.com

Table of Contents

Results in Brief

The main objective of the Fiscal Year (FY) 2025 Federal Information Security Modernization Act of 2014 (FISMA) audit was to determine whether the United States Department of Education (Department)'s overall information security program and practices are effective as they relate to federal information security requirements.

To meet this objective, Williams Adley utilized the FY 2025 Inspector General (IG) FISMA reporting metrics[1], issued on April 3, 2025, by the Office of Management and Budget (OMB). The reporting metrics provide independent assessors and IGs with a standardized framework to evaluate and report on the effectiveness and maturity of an agency's information security program.

To properly conclude on the effectiveness of the Department's information security program and practices, Williams Adley utilized a rotational strategy to select five in-scope systems[2].

The Background section of this report provides additional context on the Department, FISMA and the FY 2025 IG reporting metrics.

At the conclusion of the FY 2025 audit, Williams Adley determined that the Department's overall information security program and practices are effective as nine out of the ten FISMA domains met the requirements needed to operate at a Level 4 maturity rating or higher.[3]

Table 1 and ***Table 2*** below outline the maturity ratings assigned to the core and supplemental metrics[4], organized by security function and corresponding domain(s).

The FY 2025 Audit Results section of this report outlines how the maturity ratings and scores were calculated for each metric question and any identified conditions.

Function	Domain	Maturity Rating	Calculated Average Score
Govern	Cybersecurity Supply Chain Risk Management	Optimized	5.00
Identify	Risk and Asset Management	Managed and Measurable	4.40
Protect	Configuration Management	Optimized	5.00
Protect	Identity and Access Management	Consistently Implemented	3.33
Protect	Data Protection and Privacy	Managed and Measurable	4.00
Protect	Security Training	Optimized	5.00
Detect	Information Security Continuous Monitoring	Optimized	5.00

[1] FY 2025 IG FISMA Reporting Metrics v2.0.

[2] For the FY 2025 FISMA audit, Williams Adley selected Department Figma for Government, Access and Identity Management System, Person Authentication Service, Education Central Automated Processing System, Education Grants Platform. Refer to Appendix A for details on scope selection criteria.

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

[4] Core metrics represent the combination of Administration priorities and other highly valuable controls that must be evaluated annually. Supplemental metrics are the remainder of the FY 2025 IG FISMA controls.

Respond	Incident Response	Managed and Measurable	4.00
Recover	Contingency Planning	Optimized	5.00

Table 1 - FY 2025 Core Maturity Ratings

Function	Domain	Maturity Rating	Calculated Average Score
Govern	Cybersecurity Governance	Managed and Measurable	3.67
Identify	Risk and Asset Management	Managed and Measurable	4.00
Detect	Information Security Continuous Monitoring	Managed and Measurable	4.00

Table 2 - FY 2025 Supplemental Maturity Ratings

Although the Department has an effective information security program, Williams Adley identified a total of sixteen conditions across the ten FISMA domains — five of which resulted in a Notice of Finding and Recommendations — which represent 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. Within this report, Williams Adley offers the Department recommendations on how to address each identified root cause[5].

Williams Adley's secondary objective was to follow up on the status of outstanding recommendations to determine whether the Department has implemented their proposed corrective actions. Overall, Williams Adley determined that eight prior year recommendations were closed during the audit period and the status of the remaining open recommendations are found within Appendix B, along with their proposed target action dates.

Lastly, Williams Adley prepared the responses to the core and supplemental metric questions identified within the CyberScope questionnaire, as shown in Appendix C. All Federal agencies are required to submit their IG FISMA metric determinations into the Department of Homeland Security's CyberScope application by August 1, 2025.

[5] Williams Adley did not issue new recommendations for instances where an identified condition is related to an existing open recommendation and root cause.

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's Office of the Chief Information Officer (OCIO) advises and assists the Education 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.

The Federal Student Aid (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 does not have its own CIO but, has the Chief Technology Officer (CTO) 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.

The Department is composed of multiple offices within the Office of the Secretary, Deputy Secretary, and Office of the Under Secretary. For the Fiscal Year (FY) 2025 the Federal Information Security Modernization Act of 2014 (FISMA) audit, a representative subset of information systems within the OCIO, FSA, and Office of Finance and Operations were selected for evaluation.

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 U.S. 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, CIOs, and Inspectors General. The E-Government Act of 2002 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 E-Government Act of 2002 established that the OMB is responsible for submitting an annual report to Congress, developing, and approving the cybersecurity portions of the President's Budget, and overseeing budgetary and fiscal issues related to the agencies' use

of funds.

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

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

Fiscal Year 2025 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics

Williams Adley utilized the FY 2025 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 (IG) FISMA reporting metrics are organized around the six security functions—Govern, Identify, Protect, Detect, Respond, and Recover— as outlined in National Institute of Standards and Technology (NIST)'s cybersecurity framework.

On January 15, 2025, the OMB issued Memorandum M-25-04 ("Memorandum for the Heads of Executive Departments and Agencies: [FY] 2025 Guidance on Federal Information Security and Privacy Management Requirements") to provide instructions for meeting the FY 2025 FISMA reporting requirements.

Section VI of the Memorandum indicates that "OMB has selected a core group of metrics, representing a combination of Administration priorities and other highly valuable controls, that must be evaluated annually". The remainder of the standards and controls[6] are evaluated in metrics on a yearly cycle based on a calendar agreed to by CIGIE, the Chief Information Security Officer Council, OMB, and Cybersecurity and Infrastructure Security Agency, with a set of core metrics that must be evaluated annually and the remaining metrics that will be evaluated on a two-year cycle, beginning in FY 2023.

The FY 2025 IG FISMA Metrics introduced updated evaluation criteria, enhanced scoring guidance, and refined documentation requirements to improve consistency, risk alignment, and the overall effectiveness of cybersecurity oversight across federal agencies. Furthermore, the FY 2025 IG FISMA Metrics comprise five new supplemental metrics designed to gauge the maturity of agencies' cybersecurity governance

[6] Also referred to as "Supplemental Metrics".

practices and implementation of key components of Zero Trust Architecture. Moreover, a new FISMA function (Govern) was created for FY 2025 that includes one new domain (Cybersecurity Governance) and one existing domain (Cybersecurity Supply Chain Risk Management).

Maturity Model and Scoring Methodology

The OMB provided guidance to agency IGs or independent assessors for determining the maturity of their agencies' security programs through the publication of the FY 2025 IG 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 (govern, 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.

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[7].

[7] There are no supplemental metrics for the Protect, Respond, and Recover functions within the FY 2025 FISMA reporting metrics. As a result, IGs are instructed to consider the supplemental ratings from the FY 2023 – FY 2024 review cycle in making the final determination of program and function level effectiveness. For purposes of the FY 2025 FISMA audit, Williams Adley considered the impact of previous supplemental ratings from FY 2023 – FY 2024 on the FY 2025 scores and determined that they did not have a material impact as the Department had a mature and effective information security program during the previous FISMA cycle.

Fiscal Year 2025 Audit Results

Williams Adley assessed the effectiveness of the 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 FISMA and advanced levels (Levels 3-5) focus on the implementation, operating effectiveness, and continuous improvement of the defined policies and procedures. The following sections outline the results of our FY 2025 FISMA audit across all six FISMA functions and their ten associated domains.

Govern

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

1) Cybersecurity Governance

The Cybersecurity Governance domain focuses on establishing and maintaining the foundational policies, procedures, and organizational structures used to manage and oversee an agency's cybersecurity program, ensuring alignment with mission objectives, regulatory requirements and enterprise risk management practices.

Cybersecurity Governance – Core Reporting Metrics

Within the FY 2025 IG FISMA Metrics, the OMB did not identify any core reporting metrics specific to the Cybersecurity Governance domain.

Cybersecurity Governance – Supplemental Reporting Metrics

The OMB identified three reporting metrics as supplemental for the evaluation of a cybersecurity governance program, as outlined in ***Table 4:***

Metric Question	Topic	FY 2025 Maturity Rating	FY 2024 Maturity Rating
1	Development and maintenance of cybersecurity profiles to understand, tailor, assess, prioritize, and communicate its cybersecurity objectives.	Level 3	Not Applicable (N/A)[8]
2	Use of a cybersecurity risk management strategy to support operational risk decisions.	Level 4	N/A
3	Cybersecurity roles, responsibilities, and authorities fosters accountability, performance assessment and continuous improvement.	Level 4	N/A

Table 4 – Ratings for Supplemental Metric Questions within the Cybersecurity Governance Domain

Based on the audit procedures performed and the scores outlined in ***Table 4*** above, Williams Adley determined that the Cybersecurity Governance supplemental metrics have a calculated average score of 3.67 and a maturity rating of Level 4 (Managed and Measurable).

[8] The Cybersecurity Governance domain was introduced in the FY 2025 FISMA reporting metrics.

Metric Question Maturity Descriptions

Williams Adley concluded that the maturity rating for FISMA metric question 1 is Level 3 (Consistently Implemented), as the Department has developed, implemented, and maintained its current and target cybersecurity profiles, including assessing the gaps between the profiles. However, the Department does not consistently document the planned remediation actions to address the gaps between its current and target profiles (Condition 1).

Williams Adley concluded that the maturity rating for FISMA metric question 2 is Level 4 (Managed and Measurable), as the Department defined and consistently implemented its risk management strategy at the organizational, mission/business process, and system levels. Additionally, the Department uses qualitative and quantitative data to assess cybersecurity risk management effectiveness, dashboards, and automated tools inform adjustments to the strategy. Furthermore, the Department regularly reviews and updates the metrics, dashboards, and automated tools used to make informed adjustments to its strategy. However, it was determined that the operational status of the Education Grants Platform (EGP)[9] system is not accurately reflected within the Department's Cybersecurity Risk Scorecard (Condition 2).

Williams Adley concluded that the maturity rating for FISMA metric question 3 is Level 4 (Managed and Measurable), as the Department has defined, established, and communicated roles, responsibilities, and authorities related to cybersecurity risk management. Moreover, prior to Government reduction in force (RIF) March 2025, the Department had adequate resources that were allocated to align with its cybersecurity risk strategy. The Department did not meet a Level 5 maturity rating due to the recent RIF. Further, due to the RIF, the Department needs to reevaluate and reallocate its resources (budget, people, and tools) to ensure that the existing leadership can continue to foster a culture that is risk aware, ethical, and continually improving.

Cause, Effect, and Recommendations[10]

Williams Adley believes that the two conditions identified within the Cybersecurity Governance domain are the results of the following identified root causes and have the following effect on the Department's information security program:

- Condition 1:
    - Cause: The implementation of the Plan of Action and Milestones (POA&M) process, including the documentation of action plans, was inconsistent due to the Government RIF; specifically, the loss of Information System Owners and Information System Security Officer that were responsible for the POA&Ms process.
    - Effect: Without a clear and consistent documentation of planned remediations to address gaps between current and target profiles, the Department risks reduced accountability, misaligned priorities, and a lack of visibility into progress toward security or compliance objectives. This may hinder effective resource allocation, delay gap closure efforts, and impair the organization's ability to demonstrate due diligence to internal stakeholders and external oversight bodies.
- Condition 2:
    - Cause: Williams Adley identified that the recent shift in administration priorities and reduction in staffing and budget resources at the Department have delayed the submission and the approval of the administrative decommissioning paperwork. The administrative delay impacted the frequency in which updates are made to the Governance, Risk, and Compliance Tool (GRCT) and Cybersecurity Framework (CSF) Scorecard[11].
    - Effect: Failure to accurately reflect the operational status of a system impairs the

[9] Further details about EGP can be found in the "Other Matter Section".

[10] See criteria related to all conditions in Appendix E.

[11] Due to the recent Government RIF, EGP contract was cancelled, and the system was decommissioned.

Department's ability to maintain an accurate understanding of its risk posture and may result in outdated or incomplete security documentation, misaligned resource allocation, and inaccurate reporting.

To address the identified root causes, Williams Adley recommends that the CIO require the Department and FSA to:

- Enhance its existing standardized processes to ensure that planned remediation activities addressing gaps are clearly documented (Recommendation 1.1).
- Enhance its existing process to ensure that changes to system operational status are made accurately and timely in both the GRCT and the CSF Risk Scorecard (Recommendation 1.2).

2) Cybersecurity Supply Chain Risk Management

Cybersecurity Supply Chain Risk Management function embodies the govern program and focuses on the policies, processes, and controls implemented for identifying, assessing, and mitigating risks associated with the acquisition and use of products, information communication technology and services form external suppliers (including cybersecurity risk management, alignment with mission objectives, information security program, policies, procedures and strategy, etc.).

Cybersecurity Supply Chain Risk Management – Core Reporting Metrics

The OMB identified one reporting metric as core for the development of a cybersecurity supply chain risk management program, as outlined in ***Table 5:***

Metric Question	Topic	FY 2025 Maturity Rating	FY 2024 Maturity Rating
5	The agency ensures that products, system components, systems, and services of external providers are consistent with cybersecurity and cybersecurity supply chain requirements.	Level 5	Level 5

Table 5 – Ratings for Core Metric Questions within the Cybersecurity Supply Chain Risk Management Domain

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

Cybersecurity Supply Chain Risk Management – Supplemental Reporting Metrics

Within the FY 2025 IG FISMA Metrics, OMB did not identify any supplemental reporting metrics specific to the Cybersecurity Supply Chain Risk Management domain.

Metric Question Maturity Descriptions

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

Cause, Effect, and Recommendations
Williams Adley did not identify any conditions related to the Department's cybersecurity supply chain risk management program.

Identify

The Identify security function is comprised of the Risk and Asset Management metric domain. Based on our audit of the program area, Williams Adley determined that the Identify security domain did meet the requirements of an effective information security program.

3) Risk and Asset Management

Risk and Asset Management embodies the program and supporting processes to address the process of identifying, assessing, and managing cybersecurity risks to organizational operations and mission objectives (including mission, functions, image, and reputation), organizational assets, staff, and other organizations.

Risk and Asset Management – Core Reporting Metrics
The OMB identified five reporting metrics as core for the development of a risk and asset management program, as outlined in ***Table 6***:

Metric Question	Topic	FY 2025 Maturity Rating	FY 2024 Maturity Rating
7	Comprehensive and accurate inventory of agency information systems.	Level 4	Level 4
8	An up-to-date inventory of hardware assets.	Level 4	Level 4
9	An up-to-date inventory of software and associated licenses.	Level 4	Level 4
11	Information system security risks are adequately managed at all organization tiers.	Level 5	Level 5
12	Use technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization.	Level 5	Level 5

Table 6 – Ratings for Core Metric Questions within the Risk and Asset Management Domain

Based on the audit procedures performed and the scores outlined in ***Table 6*** above, Williams Adley determined that the Risk and Asset Management core metrics have a calculated average score of 4.40 and a maturity rating of Level 4 (Managed and Measurable).

Risk and Asset Management – Supplemental Reporting Metrics
The OMB identified one supplemental reporting metric for evaluation in FY 2025, as outlined in ***Table 7***:

Metric Question	Topic	FY 2025 Maturity Rating	FY 2024 Maturity Rating
10	Data Management inventory is developed, maintained, and tracked.	Level 4	N/A

Table 7 – Ratings for Supplemental Metric Questions within the Risk and Asset Management Domain

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

Metric Question Maturity Descriptions

Williams Adley concluded that the maturity of FISMA metric question 7 remains at Level 4 (Managed and Measurable). Williams Adley found that the Department continues to implement its defined policies and procedures to maintain a comprehensive and accurate inventory of its information systems and system interconnections, and the Department's information systems are covered by its information security continuous monitoring processes[12]. However, Williams Adley did find inconsistencies in the number of system interconnections identified within the GRCT and the System Security Plan (SSP) for the following in-scope systems[13]: Access and Identity Management System (AIMS) and Person Authentication Service (PAS) (Condition 3).

Williams Adley concluded that the maturity of FISMA metric question 8 remains at Level 4 (Managed and Measurable). Williams Adley found that the Department continues to implement its defined policies and procedures to maintain a comprehensive and accurate inventory of its hardware assets and ensures they are covered by the enterprise-wide hardware asset management capability and are subject to the monitoring processes defined within the Department's information security continuous monitoring strategy. Although the Department has an inventory of its hardware assets, Williams Adley did find missing required data elements in the hardware component inventories for four systems[14] as shown in ***Table 8*** below (Condition 4):

System Name	Missing Hardware Taxonomy Elements
AIMS	Internet Protocol (IP) Address, Hardware Model, Manufacturer Serial Number, Basic Input/Output System (BIOS) Universal Unique Identifier/Globally Unique Identifier (UUID/GUID), Media Access Control (MAC) Address(es), Date Device Added to System Boundary, and First Tier Supplier
Education Central Automated Processing System (EDCAPS)	IP Address (External), BIOS UUID/GUID, and MAC Address(es)
EGP	Identifier or Host Name, Active Directory Domain, Operating System Version, Hosting/Cloud Service Provider Contract, Asset Category, Asset Type, Hardware Make, Hardware Model, Manufacturer Serial Number, BIOS UUID/GUID, MAC Address(es), Public, Date Device Added to System Boundary, System Owner/Device Manager, Device Operator, Systems Supported, and First Tier Supplier
PAS	IP Address (Internal), Hardware Model, Manufacturer Serial Number, BIOS UUID/GUID, MAC Address(es), Date Device Added to System Boundary, and First Tier Supplier.

Table 8 – Hardware Taxonomy Exceptions List

[12] Within the context of the FY 2025 FISMA audit, the Department's Information Security Continuous Monitoring program was deemed effective.

[13] This is a repeat finding with an open Corrective Action Plan (CAP). Therefore, this will not result in a new Notice of Finding and Recommendation (NFRs).

[14] Williams Adley did not identify any significant risk related to the missing data elements. Additionally, this is a repeat finding with an open CAP and will not result in a new NFR.

Williams Adley concluded that the maturity of FISMA metric question 9 remains at 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. However, Williams Adley did find missing required data elements in the software component inventories for four systems[15] as shown in ***Table 9*** below (Condition 5):

System Name	Missing Software Taxonomy Elements
AIMS	Secure Software Development (SSD) Attestation Status, Enterprise Architecture Technology Insertion (EATI) Number, License, License Expiration, Date Software added to Inventory, and Date Software was first detected on Device
EDCAPS	Category of Software
EGP	Software/Database Version and Category of Software, Software Type, SSD Attestation Status, EATI Number, Function, Serial Identifier (ID) and License, License Expiration, Date Software added to Inventory, Date Software was first detected on Device, Primary System Boundary Cyber Security Assessment and Management (CSAM) ID, and Primary System Boundary CSAM Acronym, Device Type, Hostname/Host ID, and First Tier Supplier
PAS	Software Type, Critical Software, Category of Software, SSD Attestation Status, EATI Number, License, License Expiration, Date Software added to Inventory, and Date Software was first detected on Device

Table 9 – Software Taxonomy Exceptions List

Williams Adley concluded that the maturity of FISMA metric question 10 is Level 4 (Managed and Measurable). Williams Adley found that the Department continues to use automation to develop and maintain a centralized data inventory that includes a mapping to the hardware and software components using or storing the data from all the Department's enterprise information systems. However, the Department did not meet Level 5, due to the reoccurring hardware and software management inventory issue in metric questions 8 and 9 that would prevent the Department from maintaining an accurate centralized data inventory that includes a mapping to the hardware and software components using or storing the data from all organizational information systems.

Williams Adley concluded that FISMA metric question 11 remains at a Level 5 (Optimized) maturity. Williams Adley found that the Department has fully integrated the use of automation, wherever possible, to increase the speed, effectiveness, and efficiency of steps associated with the risk management framework.

Williams Adley concluded that FISMA metric question 12 remains at a Level 5 (Optimized) maturity, as the Department has integrated the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its cybersecurity risk management program and the ability to consume open security control assessments language into its governance, risk, and compliance processes.

Cause, Effect, and Recommendations
Williams Adley did not identify any new conditions related to the Department's risk and asset management

[15] Williams Adley did not identify any significant risk related to the missing data elements. Additionally, this is a repeat finding with an open CAP and will not result in a new NFR.

program. Conditions 3, 4, and 5 are considered repeat findings with an open CAP[16] and will not result in a new NFR. Refer to Appendix E for additional details on the associated CAP.

Protect

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

4) Configuration Management

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

For the FY 2025 FISMA audit, Williams Adley contracted with CISO Global, Inc. to perform a vulnerability assessment and penetration test of the in-scope systems. No significant issues were identified that impact the maturity determination of the Department's Configuration Management program and the results of the assessment and recommended actions to take were provided to Department Management in a separate report.

Configuration Management – Core Reporting Metrics

The OMB identified two reporting metrics as core for the development of a configuration management program, as outlined in ***Table 10***:

Metric Question	Topic	FY 2025 Maturity Rating	FY 2024 Maturity Rating
14	Use of configuration settings and common secure configurations for information systems.	Level 5	Level 5
15	Use of flaw remediation processes for managing software vulnerabilities on all network addressable IP assets.	Level 5	Level 5

Table 10 – Ratings for Core Metric Questions within the Configuration Management Domain

Based on the audit procedures performed and the scores outlined in ***Table 10*** above, Williams Adley determined that the Configuration Management core metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Configuration Management – Supplemental Reporting Metrics

Within the FY 2025 IG FISMA Metrics, OMB did not identify any supplemental reporting metrics specific to the Configuration Management domain.

Metric Question Maturity Descriptions

Williams Adley determined that FISMA metric question 14 remains at a Level 5 (Optimized) maturity, as the Department employs automation to maintain its common secure configurations tools that automatically

[16] Management indicated that the CAPs were closed. However, due to the timing of its completion, we were unable to test the corrective actions during the FY 2025 Audit.

enforce and redeploy configuration settings to systems at frequent intervals as defined by the Department, or on an event driven basis.

Williams Adley determined that FISMA question 15 remains at a Level 5 (Optimized) maturity, as the Department centrally uses automated patch management and software update tools for all applications and network devices (including mobile devices), as appropriate, where such tools are available and safe Additionally, the Department utilizes flaw remediation processes, and performs deeper analysis of software code, as needed.

Cause, Effect, and Recommendations
Williams Adley did not identify any conditions related to the Department's configuration management program.

5) Identity and Access Management
Identity and Access Management refers to identifying policies, technologies and authorized users, using credentials, and managing user access to network resources. It also emphasizes the implementation of strong authentication, role-based access controls, and continuous monitoring to reduce risks and enforce least privilege principles.

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 11***:

Metric Question	Topic	FY 2025 Maturity Rating	FY 2024 Maturity Rating
17	Use of strong authentication mechanisms (phishing-resistant multifactor authentication mechanisms (e.g., personal identity verification [PIV], Fast Identity Online [FIDO]2, or web authentication) for non-privileged users to access the organization's physical and logical assets, networks, and systems, including for remote access.	Level 3	Level 3
18	Use of strong authentication mechanisms (phishing-resistant multifactor authentication mechanisms, PIV, FIDO2, or web authentication) for privileged users to access the organization's physical and logical assets, networks, and systems, including for remote access.	Level 4	Level 4
19	Privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties.	Level 3	Level 3

Table 11 – Ratings for Core 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 core metrics have a calculated average score of 3.33 and a maturity rating of Level 3 (Consistently Implemented)[17].

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

Identity and Access Management – Supplemental Reporting Metrics
Within the FY 2025 IG FISMA Metrics, OMB did not identify any supplemental reporting metrics specific to the Identity and Access Management domain.

Metric Question Maturity Descriptions
Williams Adley determined that FISMA metric question 17 remains at a Level 3 (Consistently Implemented) maturity, as the Department did not implement strong authentication mechanisms for non-privileged users across all evaluated systems. Specifically, Williams Adley identified the following conditions[18]:

- The assessed level of assurance stated within the PAS SSP does not match the level of assurance determined within the system's Digital Identity Assessment Statement (DIAS) (Condition 6).
- The Department continued to deploy PIV-Alternative configured government furnished equipment to the Department users (Condition 7).
- The Department has not defined an enterprise requirement and guideline to govern the PIV exemption process (Condition 8)
- All 48 sampled Department and FSA new users were granted PIV exemptions (Condition 9).

Williams Adley determined that FISMA metric question 18 remains at a Level 4 (Managed and Measurable) maturity, as the Department continues to utilize strong authentication mechanisms for its privileged users, including those who can make changes to the Domain Name System and authenticate against organizational systems.

Williams Adley determined that FISMA metric question 19 remains at a maturity level 3 (Consistently Implemented) maturity, as the Department continues to execute its processes for provisioning, managing, and reviewing privileged accounts, employes restrictions on privileged user activities and ensures that their activities are logged and reviewed periodically. Williams Adley identified the following conditions:

- One out of six sampled terminated users' privileged network access was not revoked in a timely manner. Williams Adley determined that this individual's privileged network access was not revoked until four days after the individual's termination date (Condition 10).
- Three[19] out of 16 sampled privileged user accounts were created before the required access forms were signed and approved (Condition 11).
- The Department and FSA are not compliant with Event Logging (EL) 1, 2 & 3 requirements at the enterprise-level in accordance with Memorandum (M)-21-31 (Condition 12).

Cause, Effect, and Recommendations[20]
Williams Adley believes that the three new conditions (6, 10, and 11) identified within the Identity and Access Management domain are the results of the following identified root causes and have the following effect on the Department's information security program:

- Condition 6:
    - Cause: The process for updating the GRCT[21] was not properly performed to reflect the updated level of assurance determined by the PAS' most recent DIAS.
    - Effect: Due to the inconsistencies between the GRCT, the SSPs and the DIAS, a false sense of compliance or inaccurate security posture can be provided, increasing risk exposure. This misalignment can lead to the implementation of inadequate identity verification controls, potentially allowing users with insufficiently verified identities to access federal

[18] Conditions 8 and 9 also apply to metric question 18.
[19] The three privileged accounts identified are associated with the Department FIGMA for Government (EDFIGMA) system.
[20] See criteria related to all conditions in Appendix E.
[21] SSPs are generated from the content found within the GRCT.

systems or data and undermine the integrity of the risk management process.

- Condition 10:
  - Cause: The individual's privileged network access was not revoked until four days after individual's termination date due to offboarding procedures not being followed properly.
  - Effect: Failure to promptly revoke privileged network access for terminated users increases the risk of unauthorized access to critical systems and data. This could allow the terminated user or threat actors to exploit residual access rights to disrupt operations, exfiltrate sensitive information, or compromise system integrity.
- Condition 11:
  - Cause: Management granted access to EDFIGMA prior to the completion of the access form because of the immediacy of the mission critical work.
  - Effect: Granting privileged user access outside of the written process increases the potential risk of unauthorized access and compromise of sensitive information.

To address the identified root causes, Williams Adley recommends that the CIO require the Department and FSA to:

- Enhance its existing processes to ensure that updates to DIAS are correctly made to the GRCT (Recommendation 2.1).
- Ensure that stronger mechanisms are implemented to consistently enforce its process to revoke privileged network access upon employee termination in a timely manner (Recommendation 2.2).
- Develop and implement a process for properly creating, approving, and granting appropriate access to EDFIGMA users with privileged roles (Recommendation 2.3).

Conditions 7, 8, 9, and 12 are considered repeat findings with an open CAP and will not result in a new NFR. Refer to Appendix E for additional details on the associated CAP.

6) 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 and 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 2025 Maturity Rating	FY 2024 Maturity Rating
21	Use of confidentiality, integrity, and availability of PII and other sensitive data throughout the data lifecycle. Moreover, the 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, backups of data (created, protected, maintained, and tested), access to personal email, external file sharing and storage sites, and blocked personal communication applications.	Level 4	Level 4
22	Use of security controls to prevent data exfiltration and enhance network defenses.	Level 4	Level 4

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

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

Data Protection and Privacy – Supplemental Reporting Metrics
Within the FY 2025 IG FISMA Metrics, OMB did not identify any supplemental reporting metrics specific to the Data Protection and Privacy domain.

Metric Question Maturity Descriptions
Williams Adley determined that FISMA metric question 21 remains at a Level 4 (Managed and Measurable) maturity, as the Department continues to maintain its security controls to protect PII and ensures that the security controls for protecting PII and other agency sensitive data are subject to the monitoring processes defined within the Department's information security continuous monitoring strategy. However, Williams Adley identified that the Department does not employ advanced capabilities to enhance protective controls[22] (Condition 13) and encryption was not in place to protect EGP data[23] through its data lifecycle prior to it being decommissioned (Condition 14).

Williams Adley determined that FISMA metric question 22 remains at a Level 4 (Managed and Measurable) maturity, as the Department analyzes qualitative and quantitative measures to evaluate the performance of its data exfiltration and enhanced network defenses. Additionally, the Department conducted exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses. However, Williams Adley did find that the Department's data exfiltration and enhanced network defenses are not integrated into the information security continuous monitoring and incident response programs to provide near real-time monitoring of the data that is entering and exiting the network, and other suspicious inbound and outbound communications[24] (Condition 15).

Cause, Effect, and Recommendations

Conditions 13 and 15 are associated with Level 5 requirements and will not result in a new NFR.

[22] This is a Level 5 exception and will not generate an NFR.
[23] EGP was decommissioned on April 2, 2025. Therefore, Williams Adley will not issue an NFR for this finding.
[24] This is a Level 5 exception and will not generate an NFR.

Condition 14 is associated with the decommissioned system, EGP, and will not result in a new NFR.

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

Security Training – Core Reporting Metrics
The OMB identified one reporting metric as core for the development of a security training program, as outlined in ***Table 13***:

Metric Question	Topic	FY 2025 Maturity Rating	FY 2024 Maturity Rating
24	Use of assessments of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training.	Level 5	Level 5

Table 13 – Ratings for Core Metric Questions within the Security Training Domain

Based on the audit procedures performed and the scores outlined in ***Table 13*** above, Williams Adley determined that the Security Training core metric have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Security Training – No Supplemental Reporting Metrics
Within the FY 2025 IG FISMA Metrics, OMB did not identify any supplemental reporting metrics specific to the Security Training domain.

Metric Question Maturity Descriptions
Williams Adley determined that for FISMA metrics question 24, the Department remains at a Level 5 (Optimized) maturity as the Department has addressed its identified knowledge, skills, and abilities gaps through training or talent acquisition. Moreover, the Department's personnel collectively possess a training level such that the Department can demonstrate that security incidents resulting from personnel actions or inactions are being reduced over time.

Cause, Effect, and Recommendations
Williams Adley did not identify any conditions related to the Department's security training program.

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

8) 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.

Information Security Continuous Monitoring – Core Reporting Metrics
The OMB identified two reporting metrics as core for the development of an information security continuous monitoring program, as outlined in ***Table 14***:

Metric Question	Topic	FY 2025 Maturity Rating	FY 2024 Maturity Rating
26	Use of information security continuous monitoring policies and an information security continuous monitoring strategy that addresses information security continuous monitoring requirements and activities at each organizational tier.	Level 5	Level 5
28	Performance of ongoing (continuous monitoring) information system assessments to grant system authorizations, including developing and maintaining SSPs, and monitoring system security controls.	Level 5	Level 5

Table 14 – Ratings for Core Metric Questions within the Information Security Continuous Monitoring Domain

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

Information Security Continuous Monitoring – Supplemental Reporting Metrics
The OMB identified one supplemental reporting metric for evaluation in FY 2025, as outlined in ***Table 15***:

Metric Question	Topic	FY 2025 Maturity Rating	FY 2024 Maturity Rating
27	Process of monitoring and measuring the integrity and security posture of all owned and associated assets.	Level 4	N/A[25]

Table 15 – Ratings for Supplemental Metric Questions within the Information Security Continuous Monitoring Domain

Based on the audit procedures performed and the scores outlined in ***Table 15*** above, Williams Adley determined that the Information Security Continuous Monitoring 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 the FISMA metric question 26 remains at a Level 5 (Optimized) maturity, as the Department's information security continuous monitoring policies and strategy continues to be fully

[25] FISMA metric question 27 is a new supplemental question introduced as a part of the FY 2025 IG FISMA metrics.

integrated with its enterprise and supply chain risk management, configuration management, incident response, and business continuity programs. In addition, the Department demonstrated that it is using its information security continuous monitoring policies and strategy to reduce the cost and increase the efficiency of security and privacy programs.

Williams Adley determined that the FISMA metric question 27 is at a Level 4 (Managed and Measurable) maturity, as the Department has institutionalized the implementation of advanced information security continuous monitoring technologies for analysis of trends and identification of potentially adverse events and adjusts its information security continuous monitoring processes and security measures accordingly. In addition, the Department continuously verifies insights and enforces compliance throughout the lifetime of devices and virtual assets. However, the hardware and software inventory management discrepancies found in metric questions 8 and 9 impact the Department's capability to continuously verify insights and enforce compliance throughout the lifetime of devices and virtual assets.

Williams Adley identified that the FISMA metric question 28 remains at a Level 5 (Optimized) maturity, as the Department uses the results of implemented security control assessments and monitoring process to maintain ongoing authorizations of information systems, including the maintenance of SSPs. Moreover, the Department included automated analysis tools and manual expert analysis to its authorization processes to provide initial screening, data validation, and pattern recognition allowing faster and more consistent evaluations.

Cause, Effect, and Recommendations
Williams Adley did not identify any conditions related to the Department's information security continuous monitoring program.

Respond

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

9) 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 16***:

Metric Question	Topic	FY 2025 Maturity Rating	FY 2024 Maturity Rating
30	Implementation of processes for incident detection and analysis.	Level 3	Level 3
31	Implementation of processes for incident handling.	Level 5	Level 5

Table 16 – Ratings for Core Metric Questions within the Incident Response Domain

Based on the audit procedures performed and the scores outlined in ***Table 16*** above, Williams Adley determined that the Incident Response core metrics have a calculated average score of 4.00 and a maturity rating of Level 4 (Managed and Measurable).

Incident Response – Supplemental Reporting Metrics
Within the FY 2025 IG FISMA Metrics, OMB did not identify any supplemental reporting metrics specific to the Incident Response domain.

Metric Question Maturity Descriptions
Williams Adley determined that FISMA metric question 30 remains at Level 3 (Consistently Implemented), as the Department continues to implement the enterprise-wide policies, procedures, and processes for incident detection and analysis, continue to analyze potential adverse events and indicators generated by, and continue to capture and share lessons learned on the effectiveness of its incident. However, the Department has not implemented the logging requirements at maturity EL1, 2, and 3 in accordance with OMB Memorandum M-21-31 (Condition 16). Additionally, the Department is working towards implementing the logging requirements outlined within M-21-31[26].

Williams Adley identified that the FISMA metric question 31 remains a Level 5 (Optimized) maturity as the Department utilizes dynamic reconfiguration to stop attacks, misdirect attackers, and to isolate components of systems.

Cause, Effect, and Recommendations
Condition 16 is considered a repeat finding with an open CAP and will not result in a new NFR. Refer to Appendix E for additional details on the associated CAP.

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.

10) 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 one reporting metric as core for the development of a contingency planning program, as outlined in ***Table 17***:

Metric Question	Topic	FY 2025 Maturity Rating	FY 2024 Maturity Rating
33	Results of the Business Impact Analysis (BIAs) are used to guide contingency planning efforts.	Level 5	Level 5
34	Performance of information system contingency plan	Level 5	Level 5

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

	tests/exercises.		

Table 17 – Ratings for Core Metric Questions within the Contingency Planning Domain

Based on the audit procedures performed and the scores outlined in ***Table 17*** above, Williams Adley determined that the Contingency Planning core metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Contingency Planning – No Supplemental Reporting Metrics
Within the FY 2025 IG FISMA Metrics, OMB did not identify any supplemental reporting metrics specific to the Contingency Planning domain.

Metric Question Maturity Descriptions
Williams Adley determined that the maturity for FISMA metric question 33 remains at a Level 5 (Optimized) maturity, as the Department continues to integrate its BIA and asset management processes with its enterprise risk management program to improve risk identification, accurate exposure consideration, and effective risk response.

Williams Adley identified that the maturity for FISMA metric question 34 remains at a Level 5 (Optimized) maturity, as the Department performed a full recovery and reconstitution of its information systems to a known state during the audit period. In addition, the Department proactively employed defined mechanisms to disrupt or adversely affect the system or system component and tested the effectiveness of contingency planning processes.

Cause, Effect, and Recommendations
Williams Adley did not identify any conditions related to the Department's contingency planning program.

Other Matters for Consideration

During the fieldwork phase of the FY 2025 FISMA audit, Williams Adley was informed that the EGP system would be decommissioned on April 2, 2025, as a result of the contract cancelations affecting 58 organizations that were made by the Department of Government Efficiency (DOGE). As a result, Williams Adley and OIG decided that any conditions related to EGP would be included in this report strictly for awareness and information purposes but would not generate an NFR. Additionally, all EGP related conditions did not impact the Department's maturity ratings.

Additionally, on March 11, 2025, due to the new administration's reduction in force plan, the Department approximately lost 50% of its workforce including the following:

- Approximately 600 employees that accepted the voluntary resignation opportunities;
- 259 employees that accepted the deferred resignation program; and
- 313 employees that accepted the voluntary separation incentive payment.

Moreover, the new administration abruptly terminated several contracts with various vendors and organizations throughout the Department. The reduction in contracts held by other offices within the Department have the potential to affect oversight of the FSA office, support for the migrant student information exchange, and access to a digital tool used by the OCIO to analyze National Center for Education Statistics data.

Appendix A. Objectives, Scope, and Methodology

Objectives

The main objective of the Fiscal Year (FY) 2025 Federal Information Security Modernization Act of 2014 (FISMA) audit was to determine whether the Department of Education (Department)'s overall information security program and practices are effective as they relate to federal information security requirements. The secondary objective was to follow up on the status of outstanding recommendations to determine whether the Department has implemented their proposed corrective actions.

The fieldwork for the FY 2025 audit began in October 2024 and ended in June 2025. For the FY 2025 audit, the Inspector General (IG) FISMA reporting metrics required that the agency Office of Inspector General (OIG) or an independent assessor evaluate the 20 core, and 5 supplemental reporting metrics identified by the Office of Management and Budget.

To accomplish the two objectives, Williams Adley obtained an understanding of the Department's information security program and processes across the six security functions and ten associated domains, as shown in ***Table 18*** below:

Function	Domain
Govern	Cybersecurity Governance
	Cybersecurity Supply Chain Risk Management
Identify	Risk and Asset Management
Protect	Configuration Management
	Identity and Access Management
	Data Protection and Privacy
	Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Table 18 – FY 2025 IG FISMA Functions and Domains

Specifically, Williams Adley completed the below steps to meet the objectives:

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

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

- Reviewed corrective action plans for recommendations issued during the FY 2019 through FY 2024 FISMA audits.

- Tested the design and implementation of management, operational, and technical controls based on the National Institute of Standards and Technology 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 and penetration testing for in-scope Department and FSA systems, where applicable.

Scope

The FY 2025 audit covered the period July 1, 2024, to June 30, 2025, and was performed at the Department OIG's Headquarters, Williams Adley Headquarters, and remotely via Microsoft Teams.

To select the representative subset of information systems for the FY 2025 audit, Williams Adley obtained and inspected a population of 184[27] Department's FISMA reportable and operational information systems from the Department's system of record, Cyber Security Assessment and Management System (CSAM). Williams Adley reduced this population utilizing the following criterion factors:

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

This resulted in an updated population of 60 systems and Williams Adley judgmentally selected the following five (5) out of 60 systems to determine the design and effectiveness of the Department's information security program:

- Access & Identity Management System (AIMS)
- Person Authentication Service (PAS)
- Education Central Automated Processing System (EDCAPS)
- Education Grants Platform (EGP)
- Department Figma for Government (EDFIGMA)

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*).

Determining the Sample Size

Using professional judgment, Williams Adley considered the factors described below to determine sample size:

Factor	*General Effect on Sample Size*
Tolerable rate increase (decrease)	Smaller (larger)

[27] The total inventory of 184 systems was pulled as of September 17, 2024.

Assessed control risk lower (higher)	Smaller (larger)
Expected population deviation rate increase (decrease)	Larger (smaller)
Population size	Virtually no effect
Evaluation Risk	Larger if Evaluation Risk is higher

Table 19 – Sampling Methodology Factors

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).

For small populations and infrequently operating controls, according to the AICPA Audit Guide, the suggested sample size for tests of controls are as follows in ***Tables 20*** and ***21***:

Control Frequency	*Items to Test*
Quarterly (4)	2
Monthly (12)	2-4
Semimonthly (24)	3-8
Weekly (52)	5-9

Table 20 – Frequency Sampling Approach Methodology

Population Size	*Items to Test*
4	2
12	2-4
24	3-8
52	5-9
53-249	23-25
250-2000	45-50

Table 21 – Population Sampling Approach Methodology

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

FISMA Domain	Control Activity Description	Population Size	Sample Size
Risk and Asset Management	Hardware and Software Inventory Frequency	16[28]	8[29]
Identity and Access Management	EGP Access Removal for Separated Employees and Contractors	0	0
	EDCAPS Access Removal for Separated Employees and Contractors	2	2
	PAS Access Removal for Separated Employees and Contractors	5	2
	AIMS Access Removal for Separated Employees and Contractors	2	2
	EDFIGMA Access Removal for Separated Employees and Contractors	0	0
Identity and Access Management	EGP Privileged User Authorization	10	2
	EDCAPS Privileged User Authorization	37	5
	PAS Privileged User Authorization	2	2
	AIMS Privileged User Authorization	1	1
	EDFIGMA Privileged User Authorization	6	6[30]
Identity and Access Management	Personal Identity Verification Exemption	101	48[31]

[28] This represents the total occurrence of hardware and software inventory reviews performed during the audit period. Please note that the EDFIGMA system was not included in this population as cloud service providers are not required to upload the hardware and software inventory in the Governance, Risk, and Compliance Tool (GRCT).
[29] As inventories are reviewed quarterly, Williams Adley used the control frequency for quarterly occurrence. In accordance with the sampling table methodology for control frequency, we picked two sample quarters per system for the four systems included in our testing.
[30] Williams Adley selected the entire population for EDFIGMA due to the high risk associated with the EDFIGMA access provisioning process.
[31] Williams Adley expanded its sample size due to the high risk and historical issues associated with the PIV exemption process.

Configuration Management	Center for Internet Security Deviations	11	2
Data Protection and Privacy	EGP Equipment Sanitization for Separated Employees and Contractors	0	0
	EDCAPS Equipment Sanitization for Separated Employees and Contractors	2	2
	PAS Equipment Sanitization for Separated Employees and Contractors	5	2
	AIMS Equipment Sanitization for Separated Employees and Contractors	2	2
	EDFIGMA Equipment Sanitization for Separated Employees and Contractors	0	0
Incident Response	Incident Resolution Tickets	78	24

Table 22 – Sample Sizes for Operating Effectiveness Testing

Use of Computer-Processed Data

For the FY 2025 audit, Williams Adley used computer-processed data to perform its audit procedures and support the conclusions summarized in this report. This data was obtained from the Department for instances where auditors did not have rights to access the system or directly by Williams Adley via access granted by the Department.

For instances where data was provided 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. Additionally, Williams Adley had access to the Department's security information repositories, including CSAM and the FedRAMP, to perform independent verification of evidence provided by the Department.

Williams Adley concluded that the 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 (Government Accountability Office's Yellow Book). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix B. Status of Prior Year Recommendations

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

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

Based on the audit procedures for the Fiscal Year (FY) 2025 FISMA audit, Williams Adley determined that:

- One FY 2019 recommendation was closed but will not be tested until FY 2026 Audit.
- No FY 2020 recommendation was closed
- For FY 2021 and FY 2022, there were no open recommendations.
- One FY 2023 recommendation was closed.
- Six FY 2024 recommendations were closed but five will not be tested until FY 2026 Audit.

Details related to the individual prior year recommendations are found in ***Table 23*** below.

#	Description	Status	Target Action Date
FY 2019 1.4	We recommend that the Deputy Secretary require the Office of the Chief Information Officer to ensure that 51 websites are routed through a trusted internet connection or managed trusted internet protocol service.	Closed	03/31/2025
FY 2020 1.4	We recommend that the Chief Information Officer (CIO) require the Department to establish and automate procedures to ensure all Department-wide information technology (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.	Open	09/30/2025
FY 2023 4.2	We recommend that the CIO require the Department to take immediate corrective actions for establishing quality control policies, procedures, and additional processes to ensure that user onboarding, elevated and non-elevated user access forms are properly completed, tracked, and maintained for records.	Open	8/29/2025
FY 2023 4.3	We recommend that the CIO require that the Department and Federal Student Aid (FSA) to take immediate corrective actions to ensure appropriate resources and funding are available and dedicated to complete implementation of the required Event Logging 1 and EL2 event logging maturities.	Open	12/31/2027
FY 2023 1.1.3	We recommend that the CIO require the Department to implement Cyber Security Assessment and Management System motives for security control assessment testing.	Closed	7/31/2024
FY 2024 1.2.1	We recommend that the CIO require the Department and FSA to further define the oversight controls that are in the current policy to ensure all	Open	9/30/2025

	Departmental systems consistently utilize the inventory template when completing/updating the hardware inventory.		
FY 2024 1.1.1	We recommend that the CIO require the Department and FSA to capture the missing hardware data elements for each identified system and assess whether other information systems may be missing similar or related data elements.	Closed	03/31/2025
FY 2024 1.1.2	We recommend that the CIO require the Department and FSA to review and approve the Unified Servicing and Data Solution – Maximus Education Aidvantage and the Department of Education Amazon Web Services – East/West Memorandum of Understanding (MOU). Furthermore, the Department and FSA should update existing procedures and ensure all MOUs reflect the appropriate two-year review cycle.	Closed	03/31/2025
FY 2024 4.1	We recommend that CIO require the Department and FSA to require the Department and FSA to implement a process to monitor that the position risk designations are reviewed and signed prior to the security investigation.	Closed	05/31/2025
FY 2024 4.2	We recommend that CIO require the Department and FSA to implement an automation process to centrally document, track, and share risk designation and screening information.	Closed	03/31/2025
FY 2024 5.1	We recommend that CIO require the Department and FSA to reinforce their process for documenting the authorization, review, and approval of the Privileged User Access.	Closed	03/31/2025
FY 2024 5.2	We recommend that CIO require the Department and FSA to develop enhanced monitoring controls to ensure proper internal controls mechanisms and processes are strictly enforced.	Closed	03/31/2025
FY 2024 6.1	We recommend that CIO require the Departmental Principal Offices re-evaluate the use of PIV alternates/exemptions across the organization, and modify onboarding procedures, as needed, to support a new strategic direction which aligns with the Homeland Security Presidential Directive - 12.	Open	08/29/2025

Table 23 – Prior Years Recommendation Analysis

Appendix C. Responses to 2025 CyberScope Questionnaire

Metric Question	Overall
.01	*Please provide an overall Inspector General (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 the Office of Management and Budget (OMB) will include this information in the publicly available Annual Federal Information Security Modernization Act of 2014 (FISMA) Report to Congress to provide additional context for the IG's effectiveness rating of the agency's information security program. OMB may modify the response to conform with the grammatical and narrative structure of the Annual Report.*
	The primary objective of the Fiscal Year (FY) 2025 FISMA audit was to determine whether the United States Department of Education's (Department) overall information security programs and practices are effective as they relate to federal information security requirements. The secondary objective of the FY 2025 FISMA audit was to determine the effectiveness of corrective actions taken by the Department to address previously identified and issued recommendations. To determine the effectiveness of the Department's information security program, Williams Adley utilized the following criterion factors to select a judgmental sample of Department information systems: • Federal Information Processing Standards 199 Categorization: "Moderate". • New Systems added to the inventory during 2025. • High-Value Asset Systems. • Systems containing Personally Identifiable Information. • No OIG Systems. • Systems identified as Mission Critical • Combination of systems identified as "Below Risk Tolerance" within Power BI and cloud-dependent systems • Combination of Principal Offices (e.g., Office of Chief Information Officer [OCIO], Federal Student Aid [FSA]); Office of Finance and Operations and • Combination of non-cloud and cloud-dependent systems, including cloud service providers. Based on the criterion factors, Williams Adley identified a population of 60 systems and judgmentally selected five to determine the design and effectiveness of the Department's information security program. At the conclusion of the FY 2025 audit, Williams Adley determined that nine out of ten FISMA domains (Cybersecurity Governance, Risk and Asset Management, Cybersecurity Supply Chain Risk Management, Configuration Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning) were effective, and one FISMA domain, Identity and Access Management, was not effective. Overall, the Department's

	information security programs and practices were effective supporting the five in-scope systems.

Metric Question	Cybersecurity Governance
1	*To what extent does the organization develop and maintain cybersecurity profiles that are used to understand, tailor, assess, prioritize and communicate its cybersecurity objectives?*
	Consistently Implemented Williams Adley determined that the Department has defined, developed, and implemented to process to manage its current and target cybersecurity profiles. However, it was identified that the Department does not consistently document the planned remediation actions to address the gaps between its current and target profiles.
2	*To what extent does the organization use a cybersecurity risk management strategy to support operational risk decisions?*
	Managed and Measurable
3	*To what extent do cybersecurity roles, responsibilities, and authorities foster accountability, performance assessment, and continuous improvement??*
	Managed and Measurable
4	*Please provide the assessed maturity level for the agency's Govern – Cybersecurity Governance program.*
	Managed and Measurable
4.1	*Provide any additional information on the effectiveness (positive or negative) of the organization's cybersecurity governance 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 cybersecurity governance program effective*
	Taking into consideration the maturity levels assigned to the Supplemental metrics, Williams Adley concludes that the Department's cybersecurity governance program is **effective.**

Metric Question	Cybersecurity Supply Chain Risk Management
5	*To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements?*
	Optimized
6	*Please provide the assessed maturity level for the agency's Govern - Cybersecurity Supply Chain Risk Management program*
	Optimized
6.1	*Provide any additional information on the effectiveness (positive or negative) of the organization's 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.*
	Optimized Taking into consideration the maturity level assigned to the Core metric, Williams Adley concludes that the Department's cybersecurity supply chain risk management program is **effective.**

7	*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
8	*To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including Government Furnished Equipment (GFE), Internet of Things [IoT], 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
9	*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
10	*To what extent does the organization develop and maintain inventories of data and corresponding metadata for designated data types, as appropriate throughout the data lifecycle?*
	Managed and Measurable
11	*To what extent does the organization ensure that information system security risks are adequately managed?*
	Optimized
12	*To what extent does the organization use technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?*
	Optimized
13	*Please provide the assessed maturity level for the agency's Identity – Risk and Asset Management program.*
	Managed and Measurable
13.1	*Provide any additional information on the effectiveness (positive or negative) of the organization's Risk Asset and 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 Asset Management program effective?*
	Managed and Measurable Taking into consideration the maturity levels assigned to the Core and Supplemental metrics, Williams Adley concludes that the Department's risk and asset management program is **effective.**

Metric Question	Configuration Management
14	*To what extent does the organization use configuration settings/common secure configurations for its information systems?*
	Optimized
15	*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)?*
	Optimized
16	*Please provide the assessed maturity level for the agency's Protect - Configuration Management program.*

	Optimized
16.1	*Provide any additional information (positive or negative) of the organization's configuration 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 configuration management program effective?*
	Optimized Taking into consideration the maturity levels assigned to the Core metrics, Williams Adley concludes that the Department's configuration management program is **effective**.

Metric Question	Identity and Asset Management
17	*To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., Personal Identity Verification [PIV], FIDO2, or web authentication) for non-privileged users to access the organization's physical and logical assets [organization-defined entry/exit points], networks, and systems, including for remote access?*
	Consistently Implemented Williams Adley determined that the Department has consistently implemented strong authentication mechanisms for non-privileged users of the organization's facilities and networks, including for remote access, in accordance with Federal targets. For instances where it would be impracticable to use the PIV card, the organization uses an alternative token (derived PIV credential) which can be implemented and deployed with mobile devices. However, the Department did not implement strong authentication mechanisms for non-privileged users across all evaluated systems. Specifically, Williams Adley identified the following conditions: • The assessed level of assurance stated within an in-scope system's system security plan does not match the level of assurance determined within the system's Digital Identity Assessment Statement. • The Department continued to deploy PIV-Alternative configured GFEs to the Department users. • The Department has not defined an enterprise requirement and guideline to govern the PIV exemption process. • All 48 sampled Department and FSA new users were granted PIV exemptions.
18	*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 physical and logical assets [organization-defined entry/exit points], networks, and systems, including for remote access?*
	Managed and Measurable
19	*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?*
	Consistently Implemented Williams Adley determined that the Department continues to execute its processes for provisioning, managing, and reviewing privileged accounts, employees' restrictions on privileged user activities and ensures that their activities are logged and reviewed periodically. However, Williams Adley identified the following conditions:

	• The Department and the FSA did not consistently revoke network privileged access in a timely manner for one out of six sampled separated users. • Three out of 16 in-scope sampled users accounts tested for one in-scope system were created before the required access forms were signed and approved. Furthermore, the Department is not meeting privileged identity and credential management logging requirements at maturity Event Logging (EL)1, 2, and 3 in accordance with Memorandum (M)-21-31.
20	*Please provide the assessed maturity level for the agency's Protect - Identity and Access Management program.?*
	Consistently Implemented Taking into consideration the maturity levels assigned to the Core metrics, Williams Adley concludes that the Department's identity and access management program is **not effective**.
20.1	*Please 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 assigned to the Core metrics, Williams Adley concludes that the Department's identity and access management program is **not effective.**

Metric Question	Data Protection and Privacy
21	*To what extent has the organization implemented the following security controls to protect the confidentiality, integrity, and availability of its PII and other agency sensitive data, as appropriate, throughout the data lifecycle?*
	Managed and Measurable
22	*To what extent has the organization implemented security controls (e.g., DLP, IDPS, CASB, User and Entity Behavior Analytic tools, SIEM and EDR) to prevent data exfiltration and enhance network defenses?*
	Managed and Measurable
23	*Please provide the assessed maturity level for the agency's Protect - Data Protection and Privacy program.*
	Managed and Measurable
23.1	*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 metrics, Williams Adley concludes that the Department's data protection and privacy program is **effective**.

Metric Question	Security Training
24	*To what extent does the organization use an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover?*
	Optimized
25	*Please provide the assessed maturity level for the agency's Protect - Security Training program.*
	Optimized
25.1	*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 level assigned to the Core metric, Williams Adley concludes that the Department's security training program is **effective**.

Metric Question	Information Security Continuous Monitoring
26	*To what extent does the organization use information security continuous monitoring policies and an information security continuous monitoring strategy that addresses information security continuous monitoring requirements and activities at each organizational tier?*
	Optimized
27	*To what extent does the organization monitor and measure the integrity and security posture of all owned and associated assets?*
	Managed and Measurable
28	*How mature are the organization's processes for performing ongoing information (continuous monitoring) information system assessments to grant system authorizations, including developing and maintaining system security plans, and monitoring system security controls?*
	Optimized
29	*Please provide the assessed maturity level for the agency's Detect - Information Security Continuous Monitoring function.*
	Optimized
29.1	*Provide any additional information on the effectiveness (positive or negative) of the organizations information security continuous monitoring 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 information security continuous monitoring program effective?*
	Taking into consideration the maturity levels assigned to the Core and Supplemental metrics, Williams Adley concludes that the Department's information security continuous monitoring program is **effective**.

Metric Question	Incident Response
30	*To what extent has the organization implemented processes related to incident detection and analysis?*
	Consistently Implemented
31	*To what extent has the organization implemented processes related to incident handling?*

	Optimized
32.1	*Please provide the assessed maturity level for the agency's Respond - Incident Response function*
	Managed and Measurable
32	*Provide any additional information (positive or negative) of the organization's incident response 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 incident response program effective?*
	Taking into consideration the maturity levels assigned to the Core metrics, Williams Adley concludes that the Department's incident response program is **effective**.

Metric Question	Contingency Planning
33	*To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts?*
	Optimized
34	*To what extent does the organization perform tests/exercises of its information system contingency planning processes?*
	Optimized
35	*Please provide the assessed maturity level for the agency's Recover - Contingency Planning function.*
	Optimized
35.1	*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 metrics, Williams Adley concludes that the Department's contingency planning program is **effective**.

Appendix D. Department of Education's Management Response

UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF CHIEF INFORMATION OFFICER

DATE: July 25, 2025

TO: Keith Cummins
Acting Assistant Inspector General for Audit Services
Information Technology Audits and Computer Crime Investigations Office of Inspector General

FROM: Thomas N. Flagg /s/
Chief Information Officer
Department of Education

SUBJECT: Response to Federal Information Security Modernization Act of 2014 Audit of the United States Department of Education's Information Security Program and Practices Draft Report for FY 2025 Control Number A25IT0212.

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 2025*, Control Number ED-OIG/A25IT0212. 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.

Cybersecurity Governance

The ED Cybersecurity Framework (CSF) Risk Scorecard is the Department's primary tool for developing, maintaining and monitoring current and target cybersecurity profiles across all information systems and organizations within the Department. Attributes and security control for every system are assessed and quantified against the target risk profile as codified within the Information Technology (IT) Assessment, Authorization, and Monitoring (CA) Standard for all systems within the Governance, Risk, and Compliance Tool (GRCT) which is the authoritative source for the Department's system inventory of FISMA and non-FISMA reportable systems. The Current Profile, within the CSF Risk Scorecard reflects a snapshot of the Department's current cybersecurity posture, aligned to the NIST CSF. It is used as a critical input for cyber risk management and enterprise risk management, enabling the Department to identify gaps, set goals (via Target Profile), and prioritize improvements based on mission needs and

risk.

The Department's Current Profile represents existing implementation of cybersecurity activities, based on the Framework Core (functions, categories, and subcategories). It provides a snapshot of how the Department is currently managing cybersecurity risks. The Scorecard is used to inform the Secretary, Deputy Secretary, CIO, CISO, SAOP, and other Department executives as well as the AOs, ISOs, ISSOs, and Privacy team. Trend reporting occurs monthly within the CSF
Risk Scorecard to measure progress towards achieving target profile/risk appetite. The Department ensures alignment of its cybersecurity profiles with its overall risk strategy through the CA Standard in combination with the CSF Risk Scorecard and Prioritized Risk Register. The procedures and definitions for alignment of the CSF Risk Scorecard and Prioritized Risk Register to the overall risk strategy are defined in the CSF Risk Scorecard standard operating procedure (SOP). The Scorecard is used to quantify and qualify decisions on authority to operate, decommissioning, and investment through system weighting, scores and risk prioritization.

In FY 2025 Q1, the Department completed and released a new version of the CSF Risk Scorecard to align with NIST CSF v2.0, released in February 2024. The updated version provides stakeholders and executive leadership the ability to visualize risk in the context of the CSF's Govern function. The Department's accomplishments in maturing its cybersecurity governance capabilities, specifically the maturation of the Cybersecurity Framework (CSF) Risk Scorecard, have been recognized by other Federal Agencies, including OMB, as an optimized capability in managing and communicating cybersecurity risk. The Department of Commerce (DOC), Department of Justice (DOJ), Department of Transportation (DOT), The United States Agency for International Development (USAID) and Nuclear Regulatory Commission (NRC) have all requested playbooks for the development and implementation of CSF-based risk scoring capabilities in their environments based upon our constructs.

Risk Management

In addition to cybersecurity governance alignment, The ED CSF Risk Scorecard also provides the basis of the Department's risk management capability. The CSF Scorecard provides continuous monitoring, performance measurement, and risk prioritization of key metrics and risk indicators for system stakeholders, Principal Office Component (POC) leadership, and Department executive leadership on a daily, monthly, and quarterly basis. The Department continues to provide report refreshes three times daily to support more near-real time risk communication across the organization. The ED CSF Risk Scorecard also includes a daily Data Discrepancy Report (DDR) component that performs continuous validation of the information maintained within the Department's Governance Risk Compliance Tool (GRCT) to identify and correct inaccuracies.

In addition, the Department developed and released a Cyber Threat Intelligence Dashboard, integrated into the CSF Risk Scorecard, which incorporates a threat model for visualizing each system's threat susceptibility based on known vulnerabilities. This new threat model integration further advances the Department's risk management capability maturity while also ensuring its evaluation of risk reflects both known vulnerabilities and threat vectors. The Department also released an updated Prioritized Risk Register within the CSF Risk Scorecard that incorporates threat calculations in prioritizing risk remediation activities. This enhancement further empowers system owners to quickly address those weaknesses and take action to improve their system's overall security posture.

The Department continues to update and iterate its FISMA Quarterly Performance Dashboard.

Enhancements for FY 2025 include integrating with asset level Continuous Diagnostics and Mitigation (CDM) data to provide more accurate, automated hardware inventory enumeration. The updated report continues to provide extensive automation of quarterly FISMA CIO metrics capture, evaluation, and performance measurement. Additionally, this report continues to forecast the Department's FISMA performance and the effectiveness of associated risk management activities across the Department based on projected OMB Cyber Progress scores within the tool. This has allowed the Department leadership and security professionals to take a more proactive approach in FISMA compliance.

The ED Cybersecurity Policy Working Group performed their annual review of ED policy standards. The annual review included incorporating guidance and mandates from all current FY 2025 Office of Management and Budget (OMB) memoranda, Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) binding operational directives (BOD) and emergency directives (ED), as well as ED specific control overlays and enhancements.

The Department operationalized its Ongoing Security Assessment & Authorization (OSA) Program in accordance with roles and responsibilities established within the Information Technology (IT) System Security Assessment and Authorization (CA) Standard. ED has enrolled 119 FISMA reportable systems, 38 Cloud Service Providers (CSP), and 7 non-FISMA reportable subsystems into the OSA program since its adoption. The Department is also continuing efforts to leverage and enhance OSA capabilities within GRCT to streamline OSA assessment execution and program reporting. This ensures the security risks of these systems are reported on a reoccurring basis to Department management and information system stakeholders' activities are being monitored through independent security assessments. This program reporting includes establishment of a Quarterly Assessment Report within which all OSA-related activities are documented. The highlights of that report are briefed each quarter to the Authorizing Official. Also established is a new OSA CSP Independent Verification and Validation (IV&V) report that serves as an annual report of the current security posture of the CSPs leveraged within the Department to ensure they remain within the Department's risk appetite and tolerance levels. The Department has also been able to establish a pen testing capability with the development of pen testing standard operating procedures, proposed penetration testing schedule, as well as CISA AES HVA training for assessors.

The Department developed RA-05 Dashboards designed to serve as a single-pane of glass enabling information system continuous monitoring and response activities. Dashboards provide ownership and accountability for risk management activities across ED systems and are informed by vulnerability management scan data. Developed in the Department's Cyber Data Lake (CDL) tool, key information is integrated to deliver actionable insights, including CISA Known Exploitable Vulnerability (KEV), POA&M attributes, and High Value Assets (HVAs). The operation and maintenance of the RA-05 Dashboard drives processes that ensure all services within the Department's environment are scanned and assessed for risk.

Supply Chain Risk Management

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

risks.

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

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

SCRM has been a cornerstone in the implementation of the Secure Software Attestation process, working with OPM, NASA, US State Dept, Microsoft, Google, and others regarding OMB M22-18 and M-23-16 requirements and procedures. SCRM utilizes the DHS CISA Repository for Software Attestations and Artifacts (RSAA) as a centralized repository, sharing with federal agencies and reducing the burden on vendors. SCRM has assisted with the release of the ED CISO Memo: Secure Software Development Attestation Form (SSDAF) collection which aligns ED schedules to that of M-22-18 and M-23-16 to ensure all applicable critical software SSDAFs for FISMA reportable information systems have been recorded and accurately documented in the information system software inventory within GRCT. The SCRM Provenance has been updated to include automations, parsing, and the associated data of all assessment types are fed into other risk scores in a compounding capacity. Data analytics has been realized for the SCRM Team in reading the underlying data to allow for informed decision making and reporting for ED. These new capabilities address the compliances of ED against new and novel governance such as OMB M-22-18 and are used in conjunction with CISA Repository for Attestations and Artifacts (RSAA) for attestation tracking and reporting.

Configuration Management

The Department continue adopting and optimizing Zero Trust Architecture (ZTA) capabilities and solutions to enforce and monitor cybersecurity configuration standards I accordance with the OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles and the Executive Order, Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144 requirements. These efforts include but not limited to fully leveraging Software Defined Wide Area Network (SD-WAN), Cloud Access Security Broker (CASB) to continue increasing maturity in ZTA, integration with CISA Cloud Aggregation Warehouse (CLAW) and ED Cyber Data Lake (EDCDL) to achieve compliance with OMB Memorandum M-21-31 baseline requirements, maintaining Endpoint Detection & Response (EDR) capabilities for all ED systems. The Department is focused on finalizing and optimizing implementation of the TIC 3.0 architecture for ED Internet-facing systems by end of FY

2025.

The Department developed the ZTA and Trusted Internet Connection (TIC) 3.0 control mappings and overlays to NIST 800-53 rev5 controls and currently work to update cybersecurity policy and standards to integrate these overlays into the Ongoing Security Authorization (OSA) processes.

In FY 2025 The Department tailored and implemented secure configuration baselines from the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) pertaining to ED's Microsoft 365 tenant in accordance with Binding Operational Directive (BOD) 25-01. This initiative included configuring the ScubaGear tool and performing scans of the Department's Azure subscription. Post scan, The Department developed an integrated project team to work collaboratively across key stakeholder teams, including Security Architecture & Engineering (SE&A), OCIO Vulnerability Management Program (OVMP) and in-scope system technical teams. This consistent and prioritized partnership ensured accountability and drove compliance with the required SCB configurations for in-scope systems in accordance with accelerated CISA timelines. The Department refined the EATI process by implementing SCRM and Vulnerability reviews of proposed software, ensuring a strong security posture and clear risk identification before approving for use in the Department's environment. In support of enhanced Vulnerability Management activities, The Department implemented DbProtect Activity Monitoring capability. This enables real-time monitoring of database server activity, reducing risk of cyber incidents including Mean Time To Detect (MTTD).

The Department launched a FedRAMP-authorized Vulnerability Disclosure Platform (VDP), replacing a legacy email reporting process. Security Researchers supporting the Department will access this platform (hosted by Synack) via the Department VDP web page. This new platform increases efficiency in vulnerability reporting and action for impacted Department systems. Further, Security Researchers provides a common and an improved customer experience as Synack is used by many Federal VDP programs. Migration to VDP support services supports automation for our vulnerability management team and reinforces the commitment the Department has to security as a shared responsibility.

Identity and Access Management

The Department maintained its contract with a professional service provider to modernize and enhance its Enterprise Identity Credential and Access Management (ICAM) solution, which began September 1, 2022 and aligns with the OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* and the Executive Order, *Sustaining Select Efforts To Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144* requirements to meet specific cybersecurity standards and objectives. The ICAM program continues to provide improved security features and functionality which enhance the security posture of the Department. The Department continue recognizing a mature Identity Pillar as the key factor for successful implementation and utilization of enterprise Zero Trust Architecture and continue invest in the optimization and adoption of modern ICAM capabilities by all ED information systems and services.

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

greater than 90% deployment at end of FY 2024 Quarter 4, exceeding the 90% target established by OMB in FY 2023 Quarter 3. From a data encryption perspective, as of FY 2024 Quarter 4, the Department has achieved 94% data at rest (DAR) implementation compliance and 92% data in transit (DIT) compliance.

The Department's implementation of Certificate-based Authentication with Microsoft Entra ID by the Enterprise ICAM program was recognized by GSA for several best practices which have been incorporated into the FICAM Architecture implementation guidance[32] for all federal agencies. This implementation enabled the Department to adopt phishing-resistant multifactor authentication (MFA) with an X.509 certificate against its Public Key Infrastructure (PKI) directly between the Entra ID service and "relying party" applications/services across the Department. This bypasses the need for Active Directory Federation Services (ADFS) and enabled the full decommissioning of ADFS, which was completed this year.

In accordance with OMB M-22-09, the enterprise ICAM program has deployed two centrally managed phishing-resistant multifactor authentication (MFA) methods to serve as PIV-Alternate (PIV) methods when PIV or Derived PIV authentication are not available. These methods, FIDO2 security keys and Windows Hello for Business (WHfB), a Microsoft implementation of a Web Authentication-based authenticator, replace the legacy PIV-ALT single-factor authentication method (username/password), which is disallowed by M-22-09.

The Enterprise ICAM program has successfully maintained its Inter-Agency Agreement with GSA for the use of Login.gov to provide identity verification and authentication services for public users accessing Department applications and services. This includes the capability for public users to utilize several options for phishing-resistant multifactor authentication (MFA) which enables the Department to meet and exceed requirements set forth by OMB M-22-09[33]. The Enterprise ICAM program has coordinated with stakeholders across the Department to design, develop, test, and train users on its new digital identity lifecycle governance and administration (IGA) automation workflows, which automates provisioning of user account creation/disablement, birthright access, changes in user attributes and role-based access controls for individuals changing job roles/user types or leaving the Department. Additionally, this capability ensures that position risk designation forms are signed and uploaded prior to investigation dates and automates processes to centrally document, track, and share risk designation and screening information. The IGA automation workflows were deployed by the end of FY 2024. The ICAM program continues to mature IGA automation workflows to optimize management of digital identities and systems access.

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

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

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

FSA has made several enhancements to Access & Identity Management System (AIMS) and Person Authentication Service (PAS), allowing over 100 million students to better interact with FSA services, protect their accounts, and reduce the opportunity for potential fraud associated with compromised identities. The FSA Team implemented a new password requirement to comply with IRS and addended the options for users to select the use of a passphrase which greatly strengthened the factor used in multi-factor authentication that is deployed by FSA.

Data Protection and Privacy

The ED Privacy Program is managed by the Office of Planning, Evaluation and Policy Development (OPEPD) Student Privacy Policy Office (SPPO) in coordination with the Office of the Chief Information Officer (OCIO). The Department Secretary designated a Senior Agency Official for Privacy (SAOP) who is responsible and accountable for developing, implementing, and maintaining the ED Privacy Program. The Privacy Program creates and oversees privacy policies, evaluates and manages privacy risks, and ensures compliance with all applicable statutes, regulations, and policies regarding the Department's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of personally identifiable information (PII). In FY 2024, the SAOP, Kevin Herms, departed the agency. Frank Miller, Jr. now is the Acting Director of the Student Privacy Policy Office (SPPO) and the SAOP for the U.S. Department of Education. Mr. Miller leads the Department's Privacy Program and the administration of the Family Educational Rights and Privacy Act and the Protection of Pupil Rights Amendment.

During the reporting period, the Privacy Program updated the Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) templates to comply with Office of Management and Budget (OMB) Memorandum 25-21 (M-25-21), "Accelerating Federal Use of AI through Innovation, Governance, and Public Trust" in order to gauge potential impact and manage risk(s) on the privacy of individuals from the use of Artificial Intelligence (AI) related technologies. Each of these templates was fitted with additional questions related to the use of AI in order to gauge the breadth of the AI use within a Department system and to determine the impact of this use on the collection, use, processing, storage, maintenance, dissemination, and/or disclosure of PII.

In addition, the Privacy Program became a key stakeholder for the review and/or approval of proposed AI use cases and/or AI technologies that impact PII maintained by the Department. This involvement has allowed the Department to ensure that potential impacts on the privacy of individuals, potential privacy risks, and mitigation measures are analyzed before the acquisition or deployment of new AI use cases and/or technologies.

The Privacy Program also updated the Department's Cybersecurity Score Framework methodology. This update served as an enhancement to how PII elements are weighted. Privacy weights are calculated for each system to quantify different scoring thresholds based on the level of PII sensitivity of a system. If a system has a higher weight, it represents a greater risk to the Department if PII data is compromised.

Previously, the PII weight methodology was purely binary, thus not providing enough granularity to identify risk for a system. The updated PII weight methodology comprises of weighing the actual PII elements maintained within a system, based on risk, plus the amount of PII that resides within the system, to attain a more accurate weight summary to understand risk to the Department if the system is compromised.

Security Training

The Department has clear policies (i.e., ACSD-OCIO-004, *Cybersecurity Policy* and ACSDOCIO-003, *Phishing Exercise Behavioral Based Escalations*), standards (i.e., Awareness and Training [AT] Standard), and supporting procedures (i.e., Cybersecurity Training Program Consolidated Standard Operating Procedures [SOP] and Simulated Phishing Exercise SOP). These training program governance and process documents were reviewed and updated as part of program continuous monitoring. Updates to the IT Cybersecurity Awareness and Training Program Tactical Plan documented actions taken in FY 2024 and identified actions required to achieve plan goals in FY 2025 and FY 2026. The FY 2025 to FY 2026 goals include institutionalizing processes for continuous improvement, promoting awareness, and reinforcing desired behaviors. Other goals include assessing knowledge, skills, and abilities and identifying gaps to be addressed by products and services; collaborating with internal and external stakeholders to innovate the program and its resources; and finally measuring the impact of provided training.

The content of awareness and specialized security training is tailored to the demographics of the Department's workforce. This includes tailoring scenario-based learning activities in all webbased trainings to work-roles and the functions and inputs/outputs of those roles, as well as character development based upon the workforce. The FY 2025 Cybersecurity Symposium was hosted on Thursdays in October 2024. This event supports the Department's ability to provide role-based training opportunities to personnel with significant security responsibilities (SSR) and develop and maintain a cybersecurity workforce capable of actively reducing and managing risk to ED information and information systems. Over 1,100 employees and contractors participated in the event. During FY 2025 the Department further integrated the Percipio lmmersive Online Platform to the FedTalent Learning Management System. Percipio provides blended learning and improved content search capability for the ED workforce to quickly identify and immerse themselves into activities to support closing competency gaps. In FY 2025 the Department leveraged Percipio within the IT Security Role Based Training for Employees with SSR program to tailor the tool for ED employees, formatting the suggested course offerings for the six most prevalent cybersecurity workforce roles within the Department: Authorizing Official/Designating Representative (611), Program Manager (801), IT Project Manager (802), Enterprise Architect (651), and Information Systems Security Manager (722). The outcomes of the featured courses were mapped to these cyber roles, to make it simpler for the cyber workforce personnel to find courses to enhance the competencies needed for their role.

The Department launched and executed three (3) Cybersecurity and Privacy Awareness (CSPA) training courses in FY 2025 providing continual user awareness training; enabling users to define cyber risk management; educating users on identifying and recognizing threats, weaknesses, and consequences of bad actions; informing users of reporting responsibilities and expectations; and embedding users with knowledge of phishing identification and defense methodologies. The third CSPA course in FY 2025 focused on safeguarding requirements and best practices to keep ED's information safe throughout the data lifecycle and protected against emerging technologies. The course enabled users to describe how the use of social media and emerging technologies can increase risk to the department, recognize the

importance of safeguarding information and the potential impact when information is disclosed or accessed without authorization, identify common types of information that requires protection, as well as utilize best practices for data protection and reporting.

FSA's Security Services Division (SSD) has designed and implemented an updated annual Security and Disclosure Awareness training program for all Department employees and contractors who interact with Federal Tax Information (FTI) systems and data. This training equips the entire workforce with the skills and abilities to properly identify, protect, and disclose
FTI incidents. As a result, FSA can continue to receive FTI from the Internal Revenue Service (IRS), supporting the FAFSA Simplification Act and the automation of Income-Driven Repayment (IDR) certification. This automation enables faster certification and recertification for borrowers.

In FY 2025 ED continued and the use of badging incentives, presenting users with challenges to model positive behaviors. To close out the annual cyber badging program for FY 2024, ED awarded the ED Defender badge to thirty-four (34) ED employees and contractors as token of appreciation and as recognition for their dedication to protecting the Department against cyber threats by earning at all five badges that fiscal year. In FY 2025, 366 users received the Top Phish Reporter badge for reporting all FY 2024 exercise emails as suspicious, and 482 participants received cyber badges for high levels of participation in the October 2024 Symposium. As with prior years, in FY 2025 2,336 users were awarded early bird badges for completing mandatory CSPA training within the first thirty (30) days after course launch.

FSA successfully implemented the 2025 FTI Training program, achieving a 100% completion rate for both federal employees and contractors, underscoring our commitment to a highly skilled and security-aware workforce.

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

Each fiscal year ED conducts six (6) simulated phishing exercises targeting all network users. In FY 2025 an average of 97.68 % of users assessed successfully passed these exercises by properly identifying the email communication as phishing. In FY 2025, the Department continued to utilize the NIST Phish Scale into exercises. The NIST Phish Scale serves as a standardized framework designed to quantify and classify the severity and sophistication of phishing attacks.
The Phish Scale uses a rating system that is based on the message content in a phishing email. This can consist of cues that should tip users off about the legitimacy of the email and the premise of the scenario for the target audience, meaning whichever tactics the email uses would be effective for that audience.

ED also continued publishing the Simulated Phishing Program Dashboard used by OCIO IAS and POC Executive Officers, assistant secretaries, and senior leadership. 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* requirements. In FY 2025 the existing Phishing Dashboard and

separate Technical and Executive Summary Reports were combined into an enhanced Simulated Phishing Program Dashboard. These enhancements provide visibility into exercise results down to the Principal Office (PO) level, enabling PO Executive Officers at the Department the ability to identify and address potential trends through increased awareness outreach and training.

In FY 2025, ED began mapping the ED Information System Owner (ISO) and Information System Security Officer (ISSO) roles with the current version of the NIST Workforce Framework for Cybersecurity (NICE Framework) and NIST Internal Report (IR) 8355, *NICE Framework Competency Areas: Preparing a Job-Ready Cybersecurity Workforce*. The mapping was designed to create a Workforce Skills Maturity Self-assessment Tool, that would enable individuals performing in the ISO and ISSO roles to self-assess against the tasks, knowledge, and skills required by their appointment memos; ACSD-OCIO-004, *Cybersecurity Policy*; and the ED Risk Management Framework (RMF) Steps 0-6 Responsibility Matrix. The Department participated in the Federal Rotational Cyber Workforce Program designed to help Federal agencies continue to enhance their cyber workforce by developing critical cyber skills and creating environments where employees have ongoing learning and development opportunities. In FY 2025, OCIO and FSA partnered to represent the Department at the CyberCorps Scholarship for Service (SFS) Job Fair in Washington, D.C. During this time, representatives spoke with over a hundred and thirty students to provide a brief overview of the Department, talk about available internship positions, and share about the possibility of permanent positions opening at the Department. Representatives received over a hundred resumes from students interested in the program. OCIO sponsored a leadership rotation encompassing intra-agency and inter-agency development opportunities. Three leaders participated in this leadership rotation program with ninety (90) day rotations to participate in leadership development assignments.

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 6.5 published July 2, 2025). The roadmap outlines the Department's strategy for ISCM program implementation and is the core reference for all ISCM related information and provides supporting material for policies, procedures, and standards.

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

against the latest STIG published by the Department of Defense (DOD) through the DOD Cyber Exchange; and system integration into CDM tools and audit logs into EDCDL.

Incident Response

From an incident response perspective, there have been no major cybersecurity incidents across the Department in FY 2025. Additionally, automated workstreams have been documented and developed in the Department's enterprise ticket system to manage the incident response and reporting processes.

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

The Cyber Data Innovation and Services (CDIS) team, in collaboration with Splunk partners, successfully implemented IPv6 capable monitoring across ED Cyber Data Lake (EDCDL) and Splunk Cloud, enhancing support for both IPv6 native and dual-stack devices in compliance with Executive Order M-21-07. To improve data quality and workload monitoring, new technical capabilities contributed to the disabling of over 40 unneeded searches and retirement of two applications. Splunk Cloud indexers were optimized, improving average search time by 50%. Additionally, the Department extended several incident response education opportunities to system owners and SOC analysts to monitor their data better proactively for avenues of increased efficiency, potential exfiltration and overall better use of this tool by the community. The team also addressed workstation log ingest reliability with a new universal forwarder tracking dashboard and a robust recovery solution, expected to significantly reduce non-reporting workstations.

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.

FSA has made improvements across all facets of our cybersecurity framework, specifically in our ability to identify, protect, detect, respond, and recover from cyber threats. A pivotal development has been the establishment of 24/7 Security Operations Center (SOC) on-call support for weekends, ensuring continuous vigilance after hours. We've also expanded our SOC capabilities. Our communication processes have been improved through reoccurring threat intelligence meetings with our strategic partners, fostering a collaborative environment for sharing insights and learning. Furthermore, we continue tuning our threat hunt meetings to disseminate cutting-edge research and techniques, enhancing our environmental monitoring.

A key achievement in threat detection was the development of 344 MITRE ATT&CK framework-aligned alerts now fully operational in production. We've also implemented a robust new process for the

validation and tracking of OMB M-21-31 compliance.

FSA SOC improved asset monitoring & log visibility Splunk Dashboard content. This allows the FSA SOC to accurately determine and confirm logging entities for each business system. Through adoption of real-time asset visibility, FSA SOC can now attest 3 USDS systems at or near 99-100% asset visibility.

FSA Splunk Security Engineering (SE) built out and implemented business system logging for Accenture Federal Services covering FSA Cloud, NSLDS, COD, EDMAPS, FSA Partner Connect, and DCC.

FSA Splunk SE & FSA SOC implemented additional Universal Forwarder configurations against NGDC & FTII Business Systems to satisfy various log requirements for 24 NGDC & FTII FSA business systems.

Moreover, our operational briefings now place a heightened emphasis on operational security. Our internal processes have been improved. We've established robust tracking for all Change Control Board (CCB) activities, providing enhanced visibility and control over environmental modifications. A critical focus has been maintaining the currency of our cybersecurity applications, ensuring they are consistently at n or n-1 release versions.

We have successfully executed a strategic consolidation of our cybersecurity tools, improving efficiency and reducing complexity. This includes the successful decommissioning of Fortify and Qualys through the adoption of Tenable One, with WebInspect next in line for removal.

Our DevSecOps process initiatives have seen progress. We've successfully deployed Aqua Security as a SaaS solution to track security across our CI/CD pipelines (FPS, FTIM, FTIDM, and Generic). This integration improves on prior deployment of Aqua, besides, assessing security in the pipeline expedites time to reach Authority to Operate (ATO) and improves the security posture for systems and applications deployed in our AWS cloud environment.

1. Our cyber hygiene and CDM programs equally benefit from the capabilities that AquaSec brings to the environment. These accomplishments, alongside numerous other ongoing initiatives, are integral to proactive and adaptive cybersecurity strategy at FSA.

Contingency Planning

The Department conducted two Information System Contingency Plan (ISCP) Tabletop Exercise (TTX) activities in FY 2025 for system stakeholders to participate. The Department made selfservice TTX materials available for systems to use in support of conducting required CP exercises outside of the Department sponsored programming. 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.

Recommendations

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

1.1: Williams Adley recommends that Chief Information Officer require the Department and FSA should enhance its existing standardized processes to ensure that planned remediation activities addressing gaps are clearly documented.

Management's Response: The Department concurs with this recommendation and will continue this effort in FY 2026 and develop a corrective action plan by September 30, 2025.

1.2: Williams Adley recommends that Chief Information Officer requires the Department and FSA enhance its existing process to ensure that changes to system operational status are made accurately and timely in both the GRCT and the CSF Risk Scorecard.

Management's Response: The Department partially concurs with this recommendation and will continue this effort in FY 2026 and develop a corrective action plan by September 30, 2025.

2.1: Williams Adley recommends that Chief Information Officer requires the Department and FSA enhance its existing processes to ensure that updates to DIAS are correctly made to the GRCT.

Management's Response: The Department concurs with this recommendation and will continue this effort in FY 2026 and develop a corrective action plan by September 30, 2025.

2.2: Williams Adley recommends that Chief Information Officer requires the Department and FSA ensure that stronger mechanisms are implemented to consistently enforce its process to revoke privileged network access upon employee termination in a timely manner.

Management's Response: The Department concurs with this recommendation and will continue this effort in FY 2026 and develop a corrective action plan by September 30, 2025.

2.3: Williams Adley recommends that Chief Information Officer requires the FSA to develop and implement a process for properly creating, approving, and granting appropriate access to EDFIGMA users with privileged roles.

Management's Response: The Department concurs with this recommendation and will continue this effort in FY 2026 and develop a corrective action plan by September 30, 2025.

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 Acting Chief Information Security Officer, Peter Hoang at (202) 245-6923.

cc: Ray Crawford, Acting Deputy Chief Information Officer, Office of the Chief Information Officer
Peter Hoang, Director, Information Assurance Services, Office of the Chief Information Officer
Davon Tyler, Acting Chief Technology Officer, Federal Student Aid
Robert Anderson, Acting Chief Information Security Officer, Federal Student Aid
Sam Rodeheaver, Audit Liaison, Office of the Chief Information Officer
Stefanie Clay, Audit Liaison, Federal Student Aid
Bucky Methfessel, Senior Counsel for Information & Technology, Office of the General Counsel
Frank Miller, Senior Agency Official for Privacy, Office of Planning, Evaluation and Policy Development

Appendix E. Fiscal Year 2025 Conditions, Associated Criteria, and Recommendations Issued

#	FISMA Metric Domain	Condition Description	Associated Criteria	Recommendation Issued
1	Cybersecurity Governance	Williams Adley identified that the Department of Education (Department) does not consistently document the planned remediation actions to address the gaps between its current and target profiles.	The National Institute of Standards and Technology (NIST)'s Standard Publication 800-53, Security and Privacy Controls for Information Systems and Organizations, includes control CA5 which states that organizations develop a plan of actions and milestones for the system to document the planned remediation actions to correct weaknesses and deficiencies.	Williams Adley recommends that the Department's Chief Information Officer (CIO) should enhance its existing standardized processes to ensure that planned remediation activities addressing gaps are clearly documented (Recommendation 1.1).
2	Cybersecurity Governance	Williams Adley identified the operational status of the Education Grants Platform (EGP) system is not accurately reflected within the CSF Risk Scorecard. Williams Adley observed on May 7, 2025, that EGP was still operational on the CSF scorecard and the Governance, Risk, and Compliance Tool (GRCT), while the Department confirmed that EGP was decommissioned on April 2, 2025.	The Inspector General (IG) Fiscal Year (FY) 2025 Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, question 7, level 3, identifies requirements for the organization to consistently implement its policies, procedures, and processes to maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public-facing websites, and third-party systems), and system interconnections.	Williams Adley recommends that the Department's CIO require the Department to enhance its existing process to ensure that changes to system operational status are made accurately and timely in both the GRCT and the CSF Risk Scorecard (Recommendation 1.2).

3	Risk and Asset Management	Williams Adley identified inconsistencies in the number of system interconnections identified within the GRCT and the system security plan (SSP) for the following in-scope systems: Access and Identity Management System (AIMS) and Person Authentication Service (PAS).	IT Assessment, Authorization, and Monitoring (CA) Standard, dated November 15, 2024, states: CA-9 Internal System Connections (L, M, H) a. Authorize internal connections of all components or classes of components to the system. b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated. c. Terminate internal system connections after determining it no longer provides support for organizational missions or business functions or when conditions meet one or more of the following: 1. Zero trust architecture standards, guidance, and memorandums from Cybersecurity and Infrastructure Security Agency (CISA), Office of Management and Budget (OMB) or NIST; 2. Targeted responses to certain types of incidents; 3. Time-of-day restrictions on system use, if implemented; or 4. Thirty (30) minutes of session inactivity. System-level activities, established by a Virtual Private Network connection, are authorized to	Corrective Action Plan (CAP), FY 2024, 1.2.1[34]

[34] There is no new Notice of Findings and Recommendations (NFR) because of the existing CAP. See Appendix B for reference

			continue after strict user interactions have ended to support remote system patching; and d. Review at least annually (i.e., each FY) the continued need for each internal connection.	
4	Risk and Asset Management	Williams Adley identified missing required data elements in the hardware component inventories for following systems: • AIMS • Education Central Automated Processing System (EDCAPS) • EGP • PAS	IT Configuration Management (CM) Standard, dated March 19, 2025, states: CM-8 System Component Inventory (Low [L], Moderate [M], High [H] Control Overlay) a. Develop and document an inventory of system components that: 1. Accurately reflects the system; 2. Includes all components within the system; 3. Does not include duplicate accounting of components or components assigned to any other system; 4. Is at the level of granularity deemed necessary for tracking and reporting; and 5. Includes the following information to achieve system component accountability: as defined in Cybersecurity Assessment and Management (CSAM) System Information, Appendix S – Hardware Listing and System Information, Appendix T – Software Listing; not required for cloud service providers or Shared Services.	CAP, FY 2024, 1.2.1

			b. Review and update the system component inventory at a minimum quarterly.	
5	Risk and Asset Management	Williams Adley identified missing required data elements in the software component inventories for following systems: • AIMS • EGP • EDCAPS • PAS	IT CM Standard, dated March 19, 2025, states: CM-8 System Component Inventory (L, M, H Control Overlay) a. Develop and document an inventory of system components that: 1. Accurately reflects the system; 2. Includes all components within the system; 3. Does not include duplicate accounting of components or components assigned to any other system; 4. Is at the level of granularity deemed necessary for tracking and reporting; and 5. Includes the following information to achieve system component accountability: as defined in CSAM System Information, Appendix S – Hardware Listing and System Information, Appendix T – Software Listing; not required for cloud service providers or Shared Services. a. b. Review and update the system component inventory at a minimum quarterly.	CAP, FY 2024, 1.2.1
6	Identity and Access Management	Williams Adley identified that assessed level of assurance stated within the PAS SSP does	The SSP Authorization Official Standard Operating Procedures, last updated on April 19, 2024, states that SSPs are to be	Williams Adley recommends that the Department's CIO require the Department to

		not match the level of assurance determined within the system's Digital Identity Acceptance Statement (DIAS).	developed, documented, and periodically updated. In addition, the SSP for PAS, last updated on January 31, 2025, states that when there are no significant changes, the Information System Owner and Information System Security Officer must sign the agreement summary for an annual update.	enhance its existing processes to ensure that updates to DIAS are correctly made to the GRCT (Recommendation 2.1).
7	Identity and Access Management	The Department continued to deploy PIV-Alternative configured Government Furnished Equipment to the Department users.	The IT IA Standard, dated October 29, 2024, identified requirement within the Control Overlay IA-2(12) ED-01 (L, M, H) to use Homeland Security Presidential Directive (HSPD) - 12 compliant Personal Identity Verification (PIV) (including Derived PIV) as the "primary" means of authentication to Federal information systems. The Department Standard PR.AC: "Emergency PIV Alternative" Memorandum states effective sixty days from the issuance of this memorandum, April 14, 2022, "all federal employees, and contractors are required to use a PIV smartcard (badge) for authentication and access to Federal facilities and information technology (IT) systems." The "Emergency PIV Alternative" Memorandum also requires that the Department continues performing progressive communication escalation procedures with personnel identified as still using: PIV – Alternate MFA.	CAP, FY 2024, 6.1

			Federal employees and contractors using a government furnished laptop configured to authenticate without a PIV card must also submit a request in ServiceNow to convert the laptop to the standard PIV authentication configuration. In conjunction with this memorandum, within sixty days, Office of CIO (OCIO) will stop deploying laptops with PIV-Alternate configuration	
8	Identity and Access Management	The Department has not defined an enterprise requirement and guideline to govern the PIV exempt process.	The IT IA Standard, dated October 29, 2024, identified requirement within the Control Overlay IA-2(12) ED-01 (L, M, H) to use HSPD-12 compliant PIV (including Derived PIV) as the "primary" means of authentication to Federal information systems. The Department Standard PR.AC: "Emergency PIV Alternative" Memorandum states effective sixty days from the issuance of this memorandum, April 14, 2022, "all federal employees, and contractors are required to use a PIV smartcard (badge) for authentication and access to Federal facilities and IT systems." The "Emergency PIV Alternative" Memorandum also requires that the Department continues performing progressive communication escalation procedures with personnel identified as still using: PIV – Alternate MFA.	CAP, FY 2024, 6.1

			Federal employees and contractors using a government furnished laptop configured to authenticate without a PIV card must also submit a request in ServiceNow to convert the laptop to the standard PIV authentication configuration. In conjunction with this memorandum, within sixty days, OCIO will stop deploying laptops with PIV-Alternate configuration	
9	Identity and Access Management	All 48 sampled Department and Federal Student Aid (FSA) new users were granted PIV exemptions.	The IT IA Standard, dated October 29, 2024, identified requirement within the Control Overlay IA-2(12) ED-01 (L, M, H) to use HSPD-12 compliant PIV (including Derived PIV) as the "primary" means of authentication to Federal information systems. The Department Standard PR.AC: "Emergency PIV Alternative" Memorandum states effective sixty days from the issuance of this memorandum, April 14, 2022, "all federal employees, and contractors are required to use a PIV smartcard (badge) for authentication and access to Federal facilities and IT systems." The "Emergency PIV Alternative" Memorandum also requires that the Department continues performing progressive communication escalation procedures with personnel identified as still using: PIV – Alternate MFA.	CAP, FY 2024, 6.1

			Federal employees and contractors using a government furnished laptop configured to authenticate without a PIV card must also submit a request in ServiceNow to convert the laptop to the standard PIV authentication configuration. In conjunction with this memorandum, within sixty days, OCIO will stop deploying laptops with PIV-Alternate configuration	
10	Identity and Access Management	Williams Adley identified that one out of six sampled terminated users' privileged network access was not revoked in a timely manner. Williams Adley determined that this individual's privileged network access was not revoked until four days after the individual's termination date.	The IT Access Control (AC) Standard identifies requirements within AC-02 (03) Account Management (M, H Control Overlay) to: • Disable accounts within as soon as possible but no later than one (1) business day when the accounts: a. Have expired; b. Are no longer associated with a user or individual; c. Are in violation of organizational policy; or d. Have been inactive for 90 days for M systems and 30 days for H systems and High Value Assets. If no automated capability is available, manual methods must be implemented and documented in the SSP. Information System Security Officers are responsible for ensuring inactive accounts are disabled if the system cannot do so automatically.	Williams Adley recommends that the Department's CIO require the Department to ensure that stronger mechanisms are implemented to consistently enforce its process to revoke privileged network access upon employee termination in a timely manner (Recommendation 2.2).

11	Identity and Access Management	Williams Adley identified three (3)[35] out of 16 sampled privileged user accounts that were created before the required access forms were signed and approved.	The IT AC Standard identifies requirements within AC-02 Account Management (L, M, H Control Overlay) to: • Require approvals by information system owners, information systems security officer, or assigned delegate for requests to create accounts. • Create, enable, modify, disable, and remove accounts in accordance with least privilege and separation of duties, and Department policies and supporting standards, including the standards within this document. • Monitor the use of accounts.	Williams Adley recommends that the Department's CIO require FSA to develop and implement a process for properly creating, approving, and granting appropriate access to Department FIGMA for Government (EDFIGMA) users with privileged roles (Recommendation 2.3).
12	Identity and Access Management	Williams Adley identified that the Department and FSA are not compliant with Event Logging (EL) 1, 2 and 3 requirements at the enterprise-level.	OMB M-21-31, dated August 27, 2021 outlines the requirements for EL 1, 2, and 3 within Appendix A: Implementation and Centralized Access Requirements. Additionally, the Memorandum provides compliance deadlines for EL maturity, as follows: • Within one year of the date of this memorandum (August 27, 2022), reach EL1 maturity. • Within 18 months of the date of this memorandum (February 27, 2023), achieve EL2 maturity. • Within two years of the date of this memorandum (August 27, 2023), achieve EL3 maturity.	CAP, FY 2024, 4.3

[35] The three (3) privileged accounts identified are associated with the EDFIGMA system.

13	Data Protection and Privacy	Williams Adley identified that the Department does not employ advanced capabilities to enhance protective controls.	The IG FY 2025 FISMA reporting metrics, question 21, level 5 requirements: The organization employs advanced capabilities to enhance protective controls, including: • Remote wiping • Dual authorization for sanitization of media devices	Not Applicable[36]
14	Data Protection and Privacy	Williams Adley identified that encryption is not in place to protect EGP data through its data lifecycle.	The IT System and Communication (SC) Protection Standard, dated March 18, 2025, identifies requirement SC-08 Transmission Confidentiality and Integrity (M, H Control Overlay) to protect the confidentiality and integrity of transmitted information as follow: • Control Overlay SC-08 ED-01 (L): Protect the confidentiality and integrity of transmitted information. • Control Overlay SC-08(01) ED-01 (L, M, H): Encrypt all sensitive information (i.e., data) when in transit in accordance with Executive Order 14028, Improving the Nation's Cybersecurity. • Control Overlay SC-28 ED-01 (L, M, H): Protect the confidentiality and integrity all sensitive information (i.e., data) at rest in accordance with Executive Order 14028, Improving the Nation's Cybersecurity and the NIST cryptographic standards.	Not Applicable[37]

[36] This is a Level 5 exception and will not generate a Notice of Findings and Recommendations (NFR).
[37] This is an exception that was found during our audit testing; however, an NFR will not be issued since the system was decommissioned.

15	Data Protection and Privacy	Williams Adley identified that the Department's data exfiltration and enhanced network defenses are not integrated into the information security continuous monitoring and incident response programs to provide near real-time monitoring of the data that is entering and exiting the network, and other suspicious inbound and outbound communications.	The IG FY 2025 FISMA reporting metrics, question 22, level 5 outlines that the organization's data exfiltration and enhanced network defenses are fully integrated into the information security continuous monitoring and incident response programs to provide near real-time monitoring of the data that is entering and exiting the network, and other suspicious inbound and outbound communications.	Not Applicable[38]
16	Incident Response	Williams Adley identified that the Department and FSA are not compliant with EL 1, 2 & 3 requirements at the enterprise-level.	OMB M-21-31, dated August 27, 2021, outlines the requirements for EL 1, 2, and 3 within Appendix A: Implementation and Centralized Access Requirements. Additionally, the Memorandum provides compliance deadlines for EL maturity, as follows: • Within one year of the date of this memorandum (August 27, 2022), reach EL1 maturity. • Within 18 months of the date of this memorandum (February 27, 2023), achieve EL2 maturity. • Within two years of the date of this memorandum (August 27, 2023), achieve EL3 maturity.	CAP, FY 2024, 4.3

Table 24 – List of Conditions, Associated Criteria, and Recommendations Issued

[38] This is a Level 5 condition and will not generate an NFR.