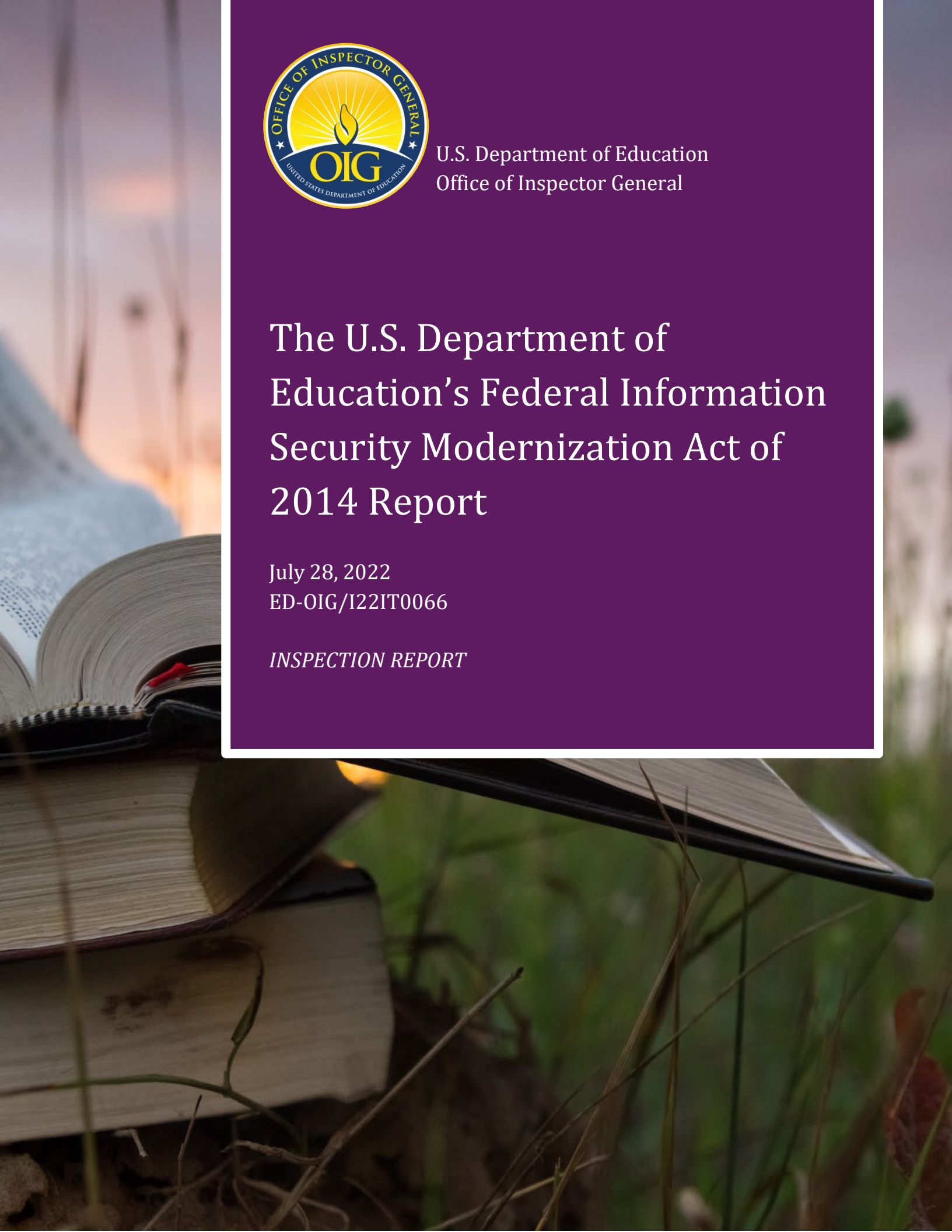


U.S. Department of Education
Office of Inspector General

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

July 28, 2022
ED-OIG/I22IT0066

INSPECTION REPORT

NOTICE

Statements that managerial practices need improvement, as well as other conclusions and recommendations in this report, represent the opinions of the Office of Inspector General. The appropriate Department of Education officials will determine what corrective actions should be taken.

In accordance with Freedom of Information Act (Title 5, United States Code, Section 552), reports that the Office of Inspector General issues are available to members of the press and general public to the extent information they contain is not subject to exemptions in the Act.

July 28, 2022

TO: Jason K. Gray
Chief Information Officer
Office of the Chief Information Officer

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

SUBJECT: Final Inspection Report
The U.S. Department of Education's Federal Information Security Modernization Act of 2014 for Fiscal Year 2022
Control Number ED-OIG/I22IT0066

Attached is the subject final Inspection report that consolidates the results of our review of the U.S. Department of Education's compliance with the Federal Information Security Modernization Act of 2014 for fiscal year 2022. We have provided an electronic copy to your audit liaison officers. We received your comments on the findings and recommendations in our draft report.

U.S. Department of Education policy requires that you develop a final corrective action plan within 30 days of the issuance of this report. 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 inspection report. Corrective actions that your office proposes and implements will be monitored and tracked through the Department's Audit Accountability and Resolution Tracking System.

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

We appreciate your cooperation during this review. If you have any questions, please contact Joseph Maranto, Director, Information Technology Audits at (202) 987-0167 or Joseph.Maranto@ed.gov.

Attachment

cc:

Cindy Marten, Deputy Secretary, Office of the Secretary and Deputy Secretary
James Kvaal, Under Secretary, Office of the Under Secretary
Richard Cordray, Chief Operating Officer, Federal Student Aid
Gary Stevens, Deputy Chief Information Officer
Steven Hernandez, Chief Information Security Officer, Office of the Chief Information Officer
Phil Rosenfelt, Deputy General Counsel, Office of General Counsel
Rob Wexler, Senior Counsel, Office of General Counsel
Margaret Glick, Chief Information Officer, Federal Student Aid
Dan Commons, Deputy Chief Information Officer, Federal Student Aid
Devin Bhatt, Deputy Chief Information Security Officer, Federal Student Aid
Samuel Rodeheaver, Audit Liaison, Office of the Chief Information Officer
Stefanie Clay, Audit Liaison, Federal Student Aid
L'Wanda Rosemond, Audit Accountability and Resolution Tracking System Administrator, Office of Inspector General

Table of Contents

Results in Brief

What We Did

Our objective was to assess the U.S. Department of Education's (Department) progress at improving the maturity of its security program and practices as required by the Federal Information Security Modernization Act of 2014 (FISMA). In fiscal year (FY) 2022, our inspection focused on 20 core metrics within the 5 security functions and the 9 associated metric domains for cybersecurity management. We evaluated the Department's security program using the 20 core Inspector General Reporting Metrics that were published for FY 2022 and issued by the Office of Management and Budget (OMB).

Our assessment for FY 2022 was significantly different from prior year audits. The FY 2022 Core IG Metrics were chosen based on alignment with Executive Order 14028, "Improving the Nation's Cybersecurity," and recent OMB guidance to agencies in furtherance of the modernization of Federal cybersecurity. Additionally, OMB Memorandum M-22-05 adjusts the timeline for the Inspectors General evaluation of agency effectiveness to align the results of the evaluation with the budget submission cycle. Historically, the evaluation of agency effectiveness by Inspectors General finished in October. This timing limited agency leadership's ability to request resources in the next budget year submissions to provide for remediations. The expectation is this change will reduce the time between issue identification, resource request and allocation.

Representatives from OMB, Federal Civilian Executive Branch Chief Information Security Officer teams, Council of the Inspectors General on Integrity and Efficiency, and the Intelligence Community agreed that these 20 Core Inspector General Metrics should provide sufficient data to determine the effectiveness of an Agency's information security program with a high level of confidence. The 20 core metrics will be evaluated annually with the remainder of the standards and controls to be evaluated on a 2-year cycle based on a calendar agreed to by the Council of the Inspectors General on Integrity and Efficiency, the Chief Information Security Officer Council, OMB, and the Cybersecurity and Infrastructure Security Agency. We focused our inspection efforts on three systems and assessed the Department's implementation of recommendations from previous reports.

We made 77 recommendations to improve the Department's cybersecurity posture in our FYs 2019, 2020, and 2021 reports. At the start of our fieldwork, there were 29 closed and 48 open recommendations. In FY 2022, we reviewed 38 open recommendations and found the Department took action to close 28 recommendations,

with 10 remaining open. Additionally, there were another 10 open recommendations that were scheduled for implementation after the close of our fieldwork.

At the completion of our FY 2022 inspection, out of 77 recommendations, 57 were closed and 20 remained open. Specifically, 11 recommendations were closed in the Configuration Management metric area and 17 recommendations were closed in the Identity and Access Management metric area. Further, 29 recommendations were closed in the Risk Management, Data Privacy and Protection, Incident Response, Information Security Continuous Monitoring, Security Training, and Contingency Planning metric areas. This demonstrates the progress that was made by the Department toward achieving an effective security program.

To answer this objective, we rated the Department's performance in accordance with OMB's guidance on the 20 metric areas required for FY 2022. These metrics represent 20 of the 66 metrics that were used to assess the Department's effectiveness for FY 2021. In September 2020, revision 5 of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations* was issued. Usually, a 1-year period is allowed for implementation of the new requirements. With the removal of 46 metric questions, for FY 2022, we were not able to test if the Department implemented these new requirements for these questions. As shown in Table 1, the metrics are grouped into five cybersecurity framework security functions that have a total of nine metric domains, as outlined in the NIST's "Framework for Improving Critical Infrastructure Cybersecurity." Table 1 also shows the significant change in the number of metric questions for each framework from FY 2021 to FY 2022. The changes in FY 2022 reduce the ability to make historical comparisons of past metric ratings.

Table 1. Cybersecurity Framework Functions, Definitions, Domains, and Number of Metric questions for FY 2021 and FY 2022

Framework Function	Definition	Domains	FY 2021 Number of Questions	FY 2022 Number of Questions
Identify	Develops the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities	Risk Management, Supply Chain Risk Management	16	6

Framework Function	Definition	Domains	FY 2021 Number of Questions	FY 2022 Number of Questions
Protect	Develops and implements the appropriate safeguards to ensure delivery of critical infrastructure services	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training	30	8
Detect	Develops and implements the appropriate activities to identify the occurrence of a cybersecurity event	Information Security Continuous Monitoring	5	2
Respond	Develops and implements the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event	Incident Response	8	2
Recover	Develops and implements the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event	Contingency Planning	7	2

Since the FY 2017 FISMA reporting process, Inspectors General were directed to use a mode-based scoring approach to assess agency maturity levels, where the most frequent level (i.e., the mode) across the questions served as the domain rating and all the metric questions were weighted equally. For FY 2022, Inspectors General were instructed to continue to use a mode-based scoring approach to assess agency maturity levels. The FY 2022 Guide instructs Inspectors General to assess the effectiveness of

20 Core IG Metrics using a maturity model approach. Figure 1 identifies the five maturity levels (with each succeeding level representing a more advanced level of implementation).

Figure 1. The 5 Maturity Levels[1]

What We Found

Based on the 20 core metrics, the Department's overall maturity rating for its security program and practices is Level 4, Managed and Measurable, which is considered to be operating at an effective level of security. In FY 2022, the Department improved its maturity rating for 20 core metrics within four security functions from Level 3, Consistently Implemented to Level 4, Managed and Measurable.[2]

[1] Maturity Levels 4 and 5 are the optimal levels to reach, with Level 4 considered to be the minimum for an effective level of security at the domain, function, and overall program.

[2] In FY 2021, the Department was scored based on 66 metric questions.

Table 2. Progress by Security Function

Security Function	FY 2021 Maturity Level	FY 2022 Maturity Level
Identify	Consistently Implemented	Consistently Implemented
Protect	Consistently Implemented	Managed and Measurable
Detect	Consistently Implemented	Managed and Measurable
Respond	Consistently Implemented	Managed and Measurable
Recover	Consistently Implemented	Managed and Measurable

In FY 2022, the Department improved its maturity rating for eight of nine metric domains. Appendix C shows the domain rating comparison from FY 2021 to FY 2022.

We determined the maturity rating for each of the Department's domains to be as follows:

Level 4—Managed and Measurable, which is considered effective for five domains: Configuration Management, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning.

Level 3—Consistently Implemented, which is considered not effective for four domains: Risk Management, Supply Chain Risk Management, Identity and Access Management, and Data Privacy and Protection.

None of the Department's domains were rated Level 1, Ad-Hoc or Level 2, Defined.

We identified findings in four of the nine metric domains, with similar conditions identified in prior reports: Configuration Management, Identity and Access Management, Data Protection and Privacy, and Incident Response.

We followed up on the status of prior year findings and 38 recommendations from the last 3 FISMA audits (FY 2019 through FY 2021) to verify that the Department has implemented corrective actions. Corrective action plans that are open or determined by the Office of Inspector General (OIG) as not completed (i.e., repeat finding with same or similar condition) at the end of fieldwork are listed in Appendix B, Status of Prior-Year Recommendations. As corrective actions are taken, OIG will continue to examine these actions and prior year open FISMA recommendations until they are completed and closed.

Our answers to the 20 core metric questions from the FY 2022 IG FISMA Metrics template used for the CyberScope report, are shown in Appendix D. All Federal agencies are required to submit their IG FISMA metric determinations into the Department of Homeland Security's CyberScope application by July 30**,** 2022.

What We Recommend

We made 10 recommendations in 4 of the 9 metric domains to assist the Department with increasing the effectiveness of its information security programs. We did not make new recommendations for any repeat and open recommendations from prior years. Refer to the details in Appendix B. The implementation of corrective action plans will help the Department fully comply with all applicable requirements of FISMA, OMB, the Department of Homeland Security, and the NIST guidance. Table 3 shows the number of recommendations we made by security function and metric domain.

Table 3 OIG Recommendations Made by Security Function and Domain

Security Function	Domains	Recommendations
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy	9
Respond	Incident Response	1

Department Comments and Our Response

We provided a draft of this report to the Department for comment. We summarize the Department's comments at the end of each finding and provide the full text of the comments at the end of the report.

Introduction

We performed our inspection in accordance with the Council of the Inspectors General for Integrity and Efficiency's Quality Standards for Inspection and Evaluation. Using the criteria outlined in the fiscal year (FY) 2022 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Metrics, our inspection focused on the evaluation of 20 core metric areas within 5 security functions and the 9 associated metric domains for cybersecurity management.

FISMA, part of the E-Government Act of 2002 (Public Law 107-347),[3] recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act of 2002, which was amended in 2014 and is commonly referred to as FISMA,[4] requires 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, contractor, or other source. The E-Government Act of 2002 also assigned specific responsibilities to the Office of Management and Budget (OMB), agency heads, chief information officers, and Inspectors General. It 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. OMB is also responsible for submitting the annual FISMA 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.

FISMA of 2014 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 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

[3] Passed by the 107th Congress and signed into law by the President in December 2002.

[4] FISMA of 2014 (Public Law 113-283), signed into law by the President in December 2014, amends Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002. As used in this report, FISMA refers both to FISMA of 2014 and to those provisions of the Federal Information Security Management Act of 2002 that were either incorporated into FISMA of 2014 or were unchanged and continue to be in effect.

monitoring in systems, increased focus on the agencies for compliance, and reporting that is more focused on the issues caused by security incidents. Furthermore, OMB regulations require Federal agencies to ensure that the appropriate officials are assigned security responsibilities and periodically review their information systems' security controls. Specifically, the agency's chief information officer is required to oversee the agency's information security program. Each agency must establish a risk-based information security program that ensures information security is practiced throughout the life cycle of each agency's systems.

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

FY 2022 Inspector General FISMA Reporting Metrics

The Inspector General FISMA metrics, in alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework, establish the information security standards and guidelines, including minimum requirements for Federal systems. NIST also developed an integrated Risk Management Framework which effectively brings together all the FISMA-related security standards and guidance to promote the development of comprehensive and balanced information security programs by agencies.

The Council of the Inspectors General on Integrity and Efficiency, OMB, and Department of Homeland Security developed the IG metrics in consultation with the Federal Chief Information Officer Council. The FY 2022 IG FISMA metrics are organized around the five information Cybersecurity Framework security functions outlined and defined in the NIST's *Framework for Improving Critical Infrastructure Cybersecurity*. Inspectors General are required to assess the effectiveness of information security programs on a maturity model spectrum, in which the foundation levels ensure that agencies develop sound policies and procedures, and the advanced levels capture the extent to which agencies institutionalize those policies and procedures. Ratings throughout the nine domains are by simple majority, where the most frequent level across the questions will serve as the overall domain rating. Further, Inspectors General determine the overall agency rating and the rating for each of the Cybersecurity Framework Functions at the maturity level.

In December 2021, OMB issued Memorandum M-22-05, *Fiscal Year 2021–2022 Guidance on Federal Information Security and Privacy Management Requirements*. The Memorandum states that in a typical year, the findings of an Inspector General assessment are released alongside annual reporting in October. However, the agency may not receive funding to remediate any problems identified until 2 or more years after the date of the report. To help remedy this situation, OMB shifted the due date of the Inspector General metrics from October to July, to better align the release of Inspector General assessments with the development of the President's Budget. Use of this reporting timeline will begin in FY 2022, starting with the core metrics.

The core metrics represent a combination of Administration priorities and other highly valuable controls, that must be evaluated annually. The remainder of the standards and controls will be evaluated in metrics on a 2-year cycle based on a calendar agreed to by the Council of the Inspectors General on Integrity and Efficiency, the Federal Chief Information Security Officer Council, OMB, and Cybersecurity and Infrastructure Security Agency. The changes do not limit the scope of OIG authority to evaluate information systems on an as-needed or ad-hoc basis.

For FY 2022, OMB selected 20 core metrics from the FY 2021 Inspector General metrics for evaluation based on their alignment with Executive Order 14028, Improving the Nation's Cybersecurity, as well as the OMB guidance outlined in M-22-05 Memorandum for the Heads of Executive Departments and Agencies, Appendix D.

U.S. Department of Education's Information Technology Investments

As of June 1, 2022, the U.S. Department of Education's (Department) FY 2022 total spending for information technology (IT) investments was estimated at over $1 billion, which included $726.5 million in spending on major IT investments (65 percent of total spending).[5] The Department's systems house millions of sensitive records on students, their parents, and others, that are used to process billions of dollars in education funding. These systems are primarily operated and maintained by contractors and are accessed by thousands of authorized people (including Department employees, contractor employees, and other third parties such as school financial aid administrators).

Department IT Systems

The Department procures most of its IT infrastructure services and items through a portfolio of multiple contracts within performance-based contracts called Portfolio of

[5] Total FY 2021 spending was $898 million.

Integrated Value Oriented Technologies (PIVOT). PIVOT is a multi-contract acquisition strategy that takes the Department's single contractor-owned, contractor-operated infrastructure and decomposes it into modular components that encourages and incentivizes service providers to focus on high-quality customer service and new product innovation.

PIVOT consists of six IT service contracts, listed below, that collectively form the core of the Department's future IT infrastructure:

- PIVOT-H—a hosting environment for Department data and systems.
- PIVOT-I—the technical management and integration of PIVOT IT services, and end-user support services.
- PIVOT-M—managed mobile device services for the Department.
- PIVOT-N—managed network services, local area network, wide area network, telecommunications, and wireless connectivity throughout the PIVOT infrastructure to facilitate all PIVOT IT services.
- PIVOT-O—oversight of all PIVOT operations to ensure that PIVOT service providers are following the operational parameters set in their contracts.
- PIVOT-P—managed print services for the Department.

In 2014, Federal Student Aid (FSA) developed a high-level strategy resulting in three service delivery models: a hybrid cloud (combination of public and private cloud); implementation of a contractor-owned, contractor-operated data center facility for legacy systems; and mainframe operations.

The Infrastructure Operations Group is responsible for planning, managing, operating, and maintaining FSA's Next Generation Data Center production and non-production environments for FSA business applications and FSA's internet and intranet network infrastructure.

FSA relies on Next Generation Data Center, a complex single vendor hybrid cloud computing environment for hosting mission critical or essential FSA Title IV application systems that support the financial aid process.

Department's Security Program

The Department's Office of the Chief Information Officer (OCIO) advises and assists the Secretary and other senior officials to ensure that the Department acquires and manages IT resources in a manner that is consistent with the requirements of the

Clinger-Cohen Act of 1996,[6] FISMA, and OMB Circular A-130. Through OCIO, the Department monitors and evaluates the contractor-provided IT services through a service-level agreement framework and develops and maintains common business solutions required by multiple program offices. OCIO is responsible for implementing the operating principles established by legislation and regulation, establishing a management framework to improve the planning and control of IT investments, and leading change to improve the efficiency and effectiveness of the Department's operations.

OCIO's Information Assurance Services team oversees the Department's IT security program and is responsible for ensuring the confidentiality, integrity, and availability of the Department's information and information resources. Information Assurance Services is responsible for the Department's compliance with FISMA and related statutes and directives. The team provides standardized information assurance and cybersecurity services and solutions. Additionally, Information Assurance Services directs the agency's security operations and incident response activities. The Director of Information Assurance Services is the designated Chief Information Security Officer, who reports directly to the Chief Information Officer, and provides overall leadership and coordination to Departmental components.

In addition to OCIO, FSA has its own Chief Information Officer, 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. FSA's Chief Information Officer core business functions are performed by four groups: the Application Development Group, the Infrastructure Operations Group, the Enterprise Architecture Group, and the Enterprise Cybersecurity Group.

Prior Years' FISMA Audit Results

During the FY 2021 FISMA audit, we made 16 recommendations in 4 of the 9 metric domains that addressed the conditions noted in the report, with most of the recommendations addressing the Protect and Respond security functions. The Department concurred with 14 recommendations and partially concurred with 2 recommendations. As of July 2022, the Department and FSA reported that they had completed corrective actions for 8 of the 16 recommendations. The Department and FSA are scheduled to complete most of the remaining corrective actions by the end of FY 2022, with some recommendations scheduled for completion at the beginning of

[6] As part of its enactment, the Clinger-Cohen Act of 1996 reformed acquisition laws and IT management of the Federal government.

2023. See Appendix B for complete details regarding prior year FISMA audit recommendations, and the status of corrective actions for FY 2019, FY 2020, and FY 2021.

Inspection Results and Findings

We had findings in four of the nine metric domains within two of the five security functions—Protect and Respond. Our findings in the metric domains Configuration Management, Identity and Access Management, Data Protection and Privacy, and Incident Response identified the same or similar conditions from prior OIG reports issued in FY 2019 through FY 2021.

Identify

The Identify security function is comprised of the Risk Management and Supply Chain Risk Management metric domains. Based on our evaluation of the two program areas, we determined that the Identify security function was consistent with the Consistently Implemented level (level 3) of the maturity model. While the Department continues to develop and strengthen its risk management and supply chain risk management programs, we noted that improvements were needed in the Department's IT inventory reporting and supply chain strategy.

Metric Domain 1—Risk Management

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

We found that for the Risk Management metric domain, the Department was at the Managed and Measurable level (level 4) for two core metric questions, the Consistently Implemented level (level 3) for three core metric questions, with an overall rating of Consistently Implemented level (level 3), which is ineffective. The Department would need to achieve a Managed and Measurable level (level 4) of security for at least three of the five core metric questions to achieve an effective Risk Management metric domain. Specifically, improvements were needed in the Department's controls over IT inventory reporting and processes. An ineffective risk management program limits the Department's ability to establish a strong process for managing information security risks.

Progress Made in FY 2022

We found the Department took several actions to improve its risk management posture, as shown in Table 4.

Table 4. Risk Management Actions Taken

Areas Improved	Actions Taken
Policies, Procedures and Standards	Established and updated its cybersecurity policy framework to align with Executive Order 14028 and NIST Special Publication (SP) 800-53, Version 5. Published cybersecurity standards designed to strengthen its risk management program that included the Information Technology Program Management Standard (1/31/2022); the Information Technology System Planning Standard (3/29/2022); the Information Technology System Security Assessment and Authorization Standard (1/31/2022); Information Technology System Risk Assessment Standard (1/31/2022); the Maintenance Standard (2/1/2022); the Executive Order 14028 Compliant Cybersecurity and Privacy Control Standards (2/2/2022); Baseline Standard OCIO-STND-01 (9/23/2021); the Plan of Action and Milestones Standard Operating Procedure, Version 2.5 (1/4/2022); the Information Technology System Services and Acquisitions Standard (1/31/2022); the Cybersecurity Framework Risk Scorecard Standard Operating Procedure, version 1.16 (1/25/2022); the FSA Enterprise Cyber Risk Committee Charter, Version 4.0 (9/1/2021); the addendum to Updated Registration and Cybersecurity Framework Risk Scoring of Unauthorized Information Systems and Services Memorandum (8/2/2021); and the Cybersecurity Framework Risk Scorecard Standard Operating Procedure (1/25/2022).
Inventory	Consistently maintained a comprehensive and accurate inventory of its information systems (including cloud systems, public-facing websites, and third-party systems) and system interconnections. Re-categorized several operational non-FISMA reportable systems as FISMA reportable. Registered several new operational cloud service providers. Enhanced its High Value Asset program with a new High Value Asset inventory. Consistently used its standard data elements to develop and maintain up to date inventory of hardware assets connected to the Department's network and used this to inform which assets can or cannot be introduced to the network.
Cyber Security Assessment and Management and System Security	Implemented its Cybersecurity Framework Scorecard 3.0 in April 2022 with NIST 800-SP 53, Revision 5, control mapping, scorecard projections, and Plan of Action and Milestones criticality scoring. Established a process for the standardization of User-Defined Risk Level Criticality determinations. Consistently implemented information security risk at the Department, mission and business process, and information system level.
Enterprise-Wide Solutions	Established and ongoing security assessment program in April 2022. The ongoing security assessment program and method of assessment replaces the older static point in time assessment model of assessment and authorization, with the ultimate objective to transition all Department systems to the ongoing security assessment program.

Areas Improved	Actions Taken
ServiceNow Service and Processes	Established processes for software installation, hardware requests (including phones, tablets, and laptops), Risk Acceptance Form requests, equipment returns, reporting of stolen devices, and loaner equipment services.

Metric Domain 2—Supply Chain Risk Management

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

The Department's Supply Chain Risk Management program remained at the Consistently Implemented level (level 3) of the maturity model because the Department did not fully implement the Supply Chain Risk Management into information security continuous monitoring practices.

Progress Made in FY 2022

We found the Department took several actions to improve its supply chain risk management posture as shown in Table 5.

Table 5. Supply Chain Risk Management Actions Taken

Areas Improved	Actions Taken
Policies, Procedures and Processes	Established and updated its cybersecurity policy framework in alignment with Executive Order 14028 and NIST SP 800-53, Revision 5, and its Information Technology System Supply Chain Risk Management Standard (3/11/2022). Consistently implemented a Department-wide information and communications technology supply chain risk management strategy to include the supply chain risk tolerance, acceptable supply chain risk mitigation strategies, and foundational practices.
Products, Systems and Components	The Department consistently implemented its policies, procedures, and processes for assessing and reviewing the supply chain-related risks associated with suppliers or contractors and system components. In addition, the Department obtained sufficient assurance, through audits and testing results, that the security and supply chain controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements, OMB policy, and applicable NIST guidance. Furthermore, the Department maintained visibility into its upstream suppliers and consistently tracked changes in suppliers.

However, the Department's practices in the Supply Chain Risk Management core metric question still did not meet the Managed and Measurable level (level 4) of maturity or an

effective level of security. The Department has not fully incorporated supplier risk evaluations, based on criticality, into its continuous monitoring practices to maintain situational awareness of its supply chain risks. Also, the Department did not provide sufficient evidence that quality control process and procedures were in place to ensure data supporting quantitative and qualitative performance metrics are obtained accurately, consistently, and in a reproducible format.

Audit follow-up and resolution is an important step towards improving the Department's cybersecurity posture. As corrective actions are taken, OIG will continue to examine these actions and prior year open FISMA recommendations until they are completed and closed. Correcting past deficiencies should improve the Department's maturity level. The FY 2022 open recommendation is as follows:

- **Recommendation 1.4**. To establish and automate procedures to ensure all Department-wide IT inventories are accurate, complete, and periodically tested for accuracy. Include steps to establish that all IT contracts are reviewed and verified for applicable privacy, security, and access provisions.

Recommendation 1.4 was reported in the FY 2020 FISMA audit report and is scheduled to be implemented by September 30, 2022.

Recommendations

There are no new recommendations for the Risk Management and Supply Chain Risk Management metric domains for this report.

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 evaluation of the four program areas, we determined that the Protect security function was consistent with the Managed and Measurable level (level 4) of the maturity model. Level 4 considered to be the minimum for an effective level of security at the domain, function, and overall program.

Metric Domain 3—Configuration Management

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

Configuration management also enables the management of system resources throughout the system life cycle. We determined that the Department's configuration management program was consistent with the Managed and Measurable level (level 4) of the maturity model.

Progress Made in FY 2022

We found the Department took the following actions to improve its configuration management posture, as shown in Table 6.

Table 6. Configuration Management Actions Taken

Areas Improved	Actions Taken
Policies, Procedures and Processes	Established and updated its cybersecurity policy framework in alignment with Executive Order 14028 and NIST SP 800-53, Revision 5. Established the Access Control Standard (2/11/2022); the Configuration Management Standard (2/11/2022); the System Services and Acquisitions Standard (1/31/2022); and the Information Technology System and Information Integrity Standard (1/31/2022). Developed and updated related standard operating procedures to clarify responsibilities and improve guidance (examples include the Enterprise Managed Network Security continuous monitoring that document and the Vulnerability Management Standard Operating Procedure). Implemented mobile device management solutions to secure mobile devices, mobile service plan services (e.g., voice, data, text messaging, machine-to-machine, etc.), mobile device management services, mobile application management services and on-site mobile life cycle professional services and associated billing services. Enforced restrictions of Bring Your Own Devices to access network resources. Enforced solutions employed for host information profile checks. Enforced security rules and geo-blocking for compliance against all devices attempting to connect. Employed solutions to actively detect rogue devices, maintaining logging account

Areas Improved	Actions Taken
	permissions, detecting unauthorized software, enforcing configuration settings, and tracking and reporting non-compliant devices.
Patch Management	In accordance with NIST SP 800-53, Revision 5, the Department's Vulnerability Management Standard Operating Procedure for PIVOT I requires that vulnerability scans are conducted for all systems. OCIO and FSA also implemented centrally managed flaw remediation policies, procedures, and processes, and ensured that patches, hotfixes, service packs, and anti-virus and malware software updates are identified, prioritized, tested, and installed in a timely manner. Tools for patch-management, anti-virus, and malware software updates are automatically distributed by the deployed tools. The Department also used continuous monitoring to monitor the performance of flaw remediations to improve patch and vulnerability management processes. OCIO established a maintenance and patching calendar to track and notify the owners of the system.
Vulnerability Disclosure	OCIO and FSA senior leadership have direct visibility of the remediation of critical vulnerabilities to assure appropriate prioritization and resource allocation reduced the significant risk of known exploited vulnerabilities. The Department released its updated Vulnerability Disclosure Policy, version 2. It also implemented strong network vulnerability enforcement on connected devices. Vulnerability information was made available via the Atlas Cyber Security Dashboards for metrics and compliance and scanning is performed on a regular basis.
ServiceNow Service and Processes	Processes were established for program change requests that include normal and emergency change requests, database support, domain name server change requests, and web and database scanning work orders.

We found that for the Configuration Management metric domain, the Department was at the Managed and Measurable level (level 4) for the two core metric questions, and subsequently the overall domain, which is an effective level of security. An effective configuration management program enhances the Department's ability to establish a strong process for managing information security risks.

Audit follow-up and resolution is an important step towards improving the Department's cybersecurity posture. As corrective actions are taken, OIG will continue to examine these actions and prior year open FISMA recommendations until they are completed and closed. Correcting past deficiencies should improve the Department's maturity level. The open recommendations in FY 2022 include:

- **FY 2019 Recommendation 2.4.** The Deputy Secretary require OCIO to ensure that 51 websites are routed through a trusted internet connection or managed trusted internet protocol service.

- **FY 2020 Recommendation 2.4.** The Chief Information Officer require the Department to establish stronger monitoring controls to enforce the management of unsupported system components and track and discontinue the use of unsupported operating systems, databases, and applications. (Incorporates a repeat recommendation)
- **Recommendation 3.3**. The Chief Information Officer require OCIO to ensure all Department websites are configured to mask personally identifiable information (PII) when used as an identifier.
- **Recommendation 3.4**. The Chief Information Officer require OCIO to enforce secure connections as required by OMB M-15-13 for all existing websites and services.

FY 2019 Recommendation 2.4 is scheduled to be implemented by September 30, 2022, FY 2020 Recommendation 2.4 is scheduled to be implemented by March 31, 2023, and Recommendations 3.3 and 3.4 are scheduled to be implemented by June 30, 2022.

Overall, the Configuration Management Program is effective with processes in place for managing information security risks. However, we found improvement was needed in the areas of patch management and secure connection protocols.

Finding 1. The Department's Configuration Management Program Needs Improvement

For the Configuration Management metric domain, although rated at the Managed and Measurable level, we found two areas where the Department and FSA can further enhance their controls for its patching process and secure connection protocols.

Patches Were Not Being Applied within the Required Timeframes

We found that the Department did not consistently apply software patches to its systems and solutions within required timeframes. In some instances, the Department and FSA continued to rely on applications that were no longer supported for patching, thus, making them vulnerable to known exploits. The Department's Vulnerability Management Standard Operating Procedure, dated January 11, 2022, is driven by criticality level and requires patching of critical vulnerabilities within 15 days of the initial detection. Likewise, high, and medium vulnerabilities are to be patched within 30 and 90 days, respectively.

To test the Department's compliance with applying patches, OIG obtained and examined the most recent vulnerability scans. OIG analyzed reports that identified critical, high, and medium vulnerabilities and identified a significant number of reports with critical, medium, and high vulnerabilities. There were 33 missing patches with a criticality designation of medium or higher (5 critical, 9 high, and 19 medium). For

example, our review of network vulnerability scan results dated March 23, 2022, disclosed two critical vulnerabilities not patched within the 15-day requirement (December 2021 and January 2022) and two high vulnerabilities not patched within the 30-day requirement (January 2022 and October 2021. The Department did not consistently implement and lacked proper controls for enforcing its vulnerability and patch management policies and standards. Failure to patch systems in a timely manner places Department systems at risk and vulnerable to malicious exploits, data leakage, damage, or exposure of sensitive information. It is imperative to assure that patches are applied in a timely manner. We reported similar conditions in our FY 2018, FY 2019, FY 2020, and FY 2021 FISMA audits.

Obsolete Protocols Being Used to Encrypt Web Server Traffic

Although the Department and FSA have made significant progress to ensure web server traffic, we found that the Department and FSA have not fully disabled and discontinued use of outdated secure connection protocols. The Department continues to use obsolete protocols to encrypt traffic, including many vulnerable to known attacks which could expose sensitive user data. In our review of the Department provided scan results, as well as our testing of the 640 uniform resource locators of the Department's website master inventory, we found instances regarding outdated protocols, which meant that:

- 4 systems were vulnerable to a secure socket layer vulnerability,
- 5 systems were vulnerable to a transport layer security vulnerability,
- 16 systems which continued to use an obsolete transport layer security protocol to encrypt web server traffic, and
- 3 websites still relied on an unsupported transport layer security protocol.

The Department and FSA need to take steps to provide assurance that obsolete encryption algorithms—such as Transport Layer Security 1.0 and 1.1—are no longer enabled as options to encrypt. NIST SP 800-52, *Guidelines for the Selection, Configuration and Use of Transport Layer Security Implementations*, states that servers that support government-only applications shall be configured to use Transport Layer Security 1.2 and begin to transition to Transport Layer Security 1.3 on or before January 1, 2024. The Department didn't have controls in place to ensure that these weak encryption protocols were disabled. Until the Department and FSA ensure that all secure connections are configured to use secure encryption protocols, systems could be vulnerable to attacks that may lead to potential exposure of sensitive data and compromise confidentiality and integrity of Departmental data. We reported a similar condition in our FY 2018, FY 2019, FY 2020, and FY 2021 FISMA audits.

Recommendations

We recommend that the Chief Information Officer require OCIO to—

1.1 Implement additional measures for patches to be prioritized and applied within established timeframes.

1.2 Establish additional oversight controls to update, remove, or replace obsolete or unsupported solutions and encryption protocols.

Department Comments

The Department agreed with Recommendations 1.1, 1.2 and committed to address these recommendations by September 30, 2022.

OIG Response

OIG will review the proposed corrective action plans to determine whether the actions will address the finding and recommendations and, if so, will validate those actions during our FY 2023 FISMA assessment.

Metric Domain 4—Identity and Access Management

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

We determined that the Department's identity and access management program was consistent with the Consistently Implemented level (level 3) of the maturity model.

Progress Made in FY 2022

We found the Department took several actions to improve its identity and access management posture, as shown in Table 7.

Table 7. Identify and Access Management Actions Taken

Areas Improved	Actions Taken
Policies and Procedures	Established and updated its cybersecurity policy framework in alignment with Executive Order 14028 and NIST SP 800-53, Version 5. Established the Information Technology System Access Control Standard (2/11/2022); the Information Technology System Audit and Accountability Standard (1/31/2022); Information Technology Identification and Authentication Standard (2/1/2022); the Information Technology System Personally Identifiable Information Processing and Transparency Standard (1/31/2022); and the Information Technology Personnel Security Standard (1/31/2022).
Strong Authentication	Consistently implemented strong authentication mechanisms for privileged and non-privileged users of the organization's facilities and networks. All privileged users use strong authentication mechanisms to authenticate to applicable organizational systems. The recertification process is being carried out across the Department as defined by the policy. Separation of duties is carried out regularly. The position designation risk process is performed, and records are maintained.
Enterprise Identity, Credential and Access Management (ICAM) solution	In December 2021, the Department's ICAM Program Office started the process of integrating all application systems with personal identity verification and multi-factor authentication to satisfy many plan of action and milestones spread across most systems at the Department. Six systems have been onboarded into ICAM process and fully integrated ICAM. In FY 2021, no systems were integrated into the process.
ServiceNow Service and Processes	Implemented the automated ServiceNow privileged user account process for providing privileged accounts. The automated ServiceNow privileged user access process works in conjunction with the automated features of CyberArk for privileged accounts. ServiceNow provides the offboarding and onboarding of employees; converting personal identity verification-alternative to standard configuration; personal identity verification exemption account enabling; creating, modifying, and removing a security group or group membership; privileged user access and removal; and account administration services.

However, the Department's practices in the Identity and Access Management core metric questions still did not meet the Managed and Measurable level (level 4) of maturity or an effective level of security. Although several improvements have been made, the Department could improve its oversight controls. Specifically, the Department's Active Directory accounts were not disabled within reasonable timeframes, risk position designations were not properly documented, and a process for tracking privileged users was not in place.

We found that for the Identity and Access Management metric domain, the Department was at the Consistently Implemented level (level 3) for two of the core metric questions and the Managed and Measurable level (level 4) for one core metric question, with an overall rating of Consistently Implemented (level 3), which is not considered effective. The Department would need to achieve a Managed and Measurable level (level 4) of security for at least two of the three core metric questions to achieve an effective Identity and Access Management metric domain.

Audit follow-up and resolution is an important step towards improving the Department's cybersecurity posture. As corrective actions are taken, OIG will continue to examine these actions and prior year open FISMA recommendations until they are completed and closed. Correcting past deficiencies should improve the Department's maturity level. The open recommendations in FY 2022 include:

Recommendation 3.3. The Chief Information Officer require OCIO to ensure all Department websites are configured to mask PII when used as an identifier.

Recommendation 4.1. The Chief Information Officer require OCIO to fully implement ICAM Strategy by established milestones to ensure the Department meets full Federal government implementation of ICAM.

Recommendation 4.4. The Chief Information Officer require OCIO to enforce a two-factor authentication configuration for all user connections to systems and applications.

Recommendation 4.5. The Chief Information Officer require OCIO to perform and evidence regularly scheduled reviews of system user accounts (both privileged and nonprivileged) to recertify and maintain each Department system's validity.

Recommendation 4.6. The Chief Information Officer require OCIO to remove terminated users' access to Department resources timely in accordance with Departmental policy.

Recommendation 4.7. The Chief Information Officer require OCIO to identify and enforce all websites to display warning banners when user's login to Departmental resources.

Recommendations 3.3, 4.1, 4.4, 4.5, 4.6 and 4.7 were reported in the FY 2021 FISMA audit report and are scheduled to be implemented by June 30, 2022.

For details, refer to Appendix B, Status of Prior-Year Recommendations.

Overall, the Identity Access Management Program is not effective with processes in place for managing information security risks. We found improvement was needed for

documenting position risk designation forms, implementing account management standards, managing privileged accounts, and controls over database management.

Finding 2. The Department's Identity Access Management Program Needs Improvement

We determined the Department and FSA's controls needed improvement for implementing properly completed and signed position designation risk forms; consistently implementing its own account and authenticator management standards; and properly maintaining, tracking, and managing privileged users. An ineffective identity and access management program limits the Department's ability to identify users and manage user access to its network resources properly and securely.

Position Risk Designation Forms Not Properly Documented

The Department and FSA did not properly oversee the process of completing and signing the position risk designation form by the Contracting Officer Representative. We judgmentally selected 35 users (24 privileged and 11 nonprivileged) and requested the position risk designation form for each user. For 31 of the 35 position risk designation forms, the Department and FSA could not provide evidence that these forms were signed and properly completed by the Contracting Officer Representative. NIST SP 800-53, Revision 5, specifies that the Position Risk Designation control should (1) assign a risk designation to all organizational positions; (2) establish screening criteria for individuals filling those positions; and (3) review and update position risk designations within an organization-defined frequency. Without evidence that the Office of Personnel Management's Position Designation Tool is properly completed and signed, there is an increased risk positions will not be properly designated based on risk and national security position duty requirements prior to releasing the contract solicitation. We reported similar conditions in the FY 2021 FISMA audit.

Account Management Standards Not Consistently Implemented

The Department did not consistently implement its account and authenticator management standards. Specifically, the Department password and account deactivation policies were not enforced. As of May 13, 2022, the Department reported 9,241 active accounts in its active directory. Although the 9,241 active accounts had a password expiration of 90 days, we found that 171 did not change their password within the required timeframe. In addition, we found 2,847 of the 9,241 accounts were not disabled after 90 days of inactivity.

We also examined a sample of 22 departed users to determine whether the Department successfully disabled the selected user's active directory account. We found that active directory accounts for 4 of 22 sampled users were not disabled accordingly. We reported similar conditions in our FY 2019 and FY 2020 FISMA audits.

The Department completed a corrective action plan based on the FY 2020 audit and acknowledged there were active directory accounts that were not in compliance. They also stated that an account reconciliation was performed to verify whether the Department's policies are being followed. Subsequently, the Departmental policy was updated to align with NIST SP 800-53, Revision 5. However, we continued to find similar issues with the Department's password expiration and the disabling of accounts.

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, dated September 2020, instructs agencies to disable accounts within an organization-defined time period. The Department's Information Technology System Access Control Standard dated February 11, 2022, Section 2.2.3 states, that accounts are to be disabled as soon as possible, but no later than one 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 low and moderate systems and 30 days for high systems and [High Value Assets]. If no automated capabilities are available, manual methods must be implemented and documented in the system security plan. The Information Systems Security Officer is responsible for ensuring inactive accounts are disabled if the system cannot do so automatically.

FSA Did Not Fully Implement a Process to Manage Privileged Accounts

CyberArk is the Department standard for accessing systems at an elevated level, and for enforcing the Department policy for privileged accounts. CyberArk and ServiceNow provide automated mechanisms for managing privileged accounts. FSA produces a monthly vendor employee report (that includes contractors) that identifies contractor accounts with privileged user permissions. We judgmentally selected 24 privileged users with access to the Enterprise Data Management and Analytics Platform Service and determined that FSA did not properly maintain, track, and manage privileged users in CyberArk. Specifically, we found 10 of the 24 selected privileged users accounts were not maintained, tracked, and managed in CyberArk. The 10 accounts that we identified were privileged contractor accounts that were not entered, maintained, or tracked into CyberArk.

NIST SP 800-53, Revision 5, states agencies are to define and document the types of accounts allowed and specifically prohibited for use within the system, assign account managers, require assignment of defined prerequisites and criteria for group and role

membership, specify authorized users of the system and the group and role membership, and access authorizations (i.e., privileges) and defined attributes for each account and monitor the use of those account.

Without accurate accounting, tracking, and reviewing of privileged users accessing Departmental systems and its resources, the Department is at increased risk of a compromise of its systems and data.

Controls Over Database Management Were Not Secured

We performed assessments that identified vulnerabilities, configuration errors, and access issues for databases included in two of the three systems reviewed. Specifically, the vulnerability scans identified significant security weaknesses that the Department and FSA need to address to better safeguard data stored in their databases. Scans of databases associated with these systems identified 31 high vulnerabilities, 45 medium vulnerabilities, and 19 low vulnerabilities. Specifically, we found that security parameters were not correctly set; permissions, privileges, and roles were incorrectly assigned; configurations were improper; failed login attempts and password parameters were incorrectly set; and audit data records were not encrypted.

The Department and FSA have not consistently implemented the necessary controls to ensure that their databases were protected. We shared the vulnerabilities with the Department and FSA for remediation. NIST SP 800-53, Revision 5, provides guidelines for selecting and specifying security controls for organization and information systems supporting the executive agencies of the Federal government to meet the requirements of Federal Information Processing Standards Publication 200, *Minimum Security Requirement for Federal Information Systems*. This includes access control, identification and authorization, system and information integrity, and system and communications protection. By allowing these vulnerabilities to exist, the Department increases the risk that unauthorized individuals can access or alter the data. We reported similar conditions in our FY 2018, FY 2019, and FY 2020, FY 2021 FISMA audits.

Recommendations

We recommend that the Chief Information Officer require OCIO to—

2.1 Ensure the Contracting Officer Representative sign, complete, and maintain Position Risk Designation forms for background investigations.

2.2 Review active directory user accounts to enforce policy compliance for password expiration and account deactivation.

2.3 Remove terminated users' access to Department resources in accordance with Departmental policy.

2.4 Establish and enforce a policy to maintain and track all privileged accounts in an authorized Privileged Access Management System(s).

2.5 Establish and enforce a corrective action plan to monitor and remediate identified database vulnerabilities.

Department Comments

The Department agreed with Recommendations 2.1 and, 2.4 and partially agreed with 2.2, 2.3, 2.5 and committed to address these recommendations by September 30, 2022.

For recommendation 2.2, the Department partially agreed with the password expiration section of the finding. For the accounts OIG identified as not disabled after inactivity, the Department clarified that these accounts were reactivated during a system migration. The Department further clarified that the reactivation was done by a system administrator using an administrator password resulting in low risk. The Department plans to do additional research and develop corrective actions by September 30, 2022.

For recommendation 2.3, The Department partially agreed and stated that the account reactivations were attributable to system administrator actions necessary for a system migration and will need to be documented in policy, as well as establishing a process to document and retaining these procedures. The Department plans to develop a corrective action plan by September 30, 2022.

For recommendation 2.5, the Department partially agreed and stated that three of the findings identified by the OIG were remediated during the 30-day required timeframe. The Department further clarified that its scanning policy follows and complies with the Defense Information Systems Agency Security Technical Implementation Guides, while the OIG used a standard industry accepted tool for FISMA policies for performing database scans and identified additional findings. Of these remaining findings the Department believes they will be resolved through evaluating vendor configurations against the Department's STIG Policy. FSA will develop a corrective action plan by September 30, 2022 to address the recommendation.

OIG Response

For Recommendation 2.2 and 2.3, the Department needs to ensure that account reactivation during the migration process is documented in policy, as well as identifying what documentation needs to be retained to verify that the process was followed. For 2.5, OIG will review the actions and scans performed by FSA.

For all recommendations, OIG will examine the proposed corrective action plans to determine whether the actions will address the finding and recommendations and, if so, will validate those actions during our FY 2023 FISMA assessment.

Metric Domain 5—Data Protection and Privacy

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

We determined that the Department's data protection and privacy program was consistent with the Consistently Implemented level (level 3) of the maturity model, although some improvements have been made. Improvements are needed for this program because the Department's process for completing supporting sanitization of digital media was not fully implemented. An ineffective data protection and privacy program limits the Department's ability to protect the privacy of individuals' PII collected, used, maintained, shared, and disposed of by programs and information systems.

Progress Made in FY 2022

As shown in Table 8, we found that the Department took several actions to improve its data protection and privacy program, especially in the areas of policies and procedures, roles and responsibilities, and data protection security controls and enhancements.

Table 8. Data Protection and Privacy Actions Taken

Areas Improved	Actions Taken
Policies and Procedures	Established and updated its cybersecurity policy framework in alignment with Executive Order 14028 and NIST SP 800-53, Version 5. Established the Information Technology System and Information Integrity Standard (1/31/2022); the Information Technology System and Communications Protection Standard (1/31/2022); the Information Technology System Personally Identifiable Information Processing and Transparency Standard (1/31/2022); Information Technology Personnel Security Standard (1/31/2022); and the Information Technology System Media Protection Standard (1/31/2022).

Areas Improved	Actions Taken
Roles and Responsibilities	The Senior Agency Official for Privacy made significant improvements to the privacy program by hiring two new privacy specialists (one senior privacy specialist and one intermediate privacy specialist) and implementing a new case management system. The privacy program has established a bi-weekly meeting with OCIO to coordinate the Department's implementation of the privacy-related elements of NIST SP 800-53, Revision 5. Additionally, the privacy program regularly presents at the regularly scheduled cybersecurity workshop on a variety of topics related to privacy policies and procedures.
Data Protection Security Controls and Enhancements	The Student Privacy Policy Office is acquiring a new case management system that will be used for all elements of the privacy compliance process, including document submission, tracking, workflow, inventory, review, and approval. The new system, which is expected to be deployed during FY 2022, will improve the privacy program's ability to track and measure our work overtime. The Department developed and implemented an internal repository that tracks and manages all the Department's privacy threshold analyses, privacy impact assessments, and system of records notices for all its systems. The new repository has enhanced the quality and timeliness of privacy documentation to plan for milestones in the system development process and avoid authorization to operate lapses.

However, the Department's practices in all metric questions still did not meet the Managed and Measurable level (level 4) of maturity for an effective level of security. The Department would need to achieve a Managed and Measurable level of security for at least one of the two metric questions, with the other being Consistently Implemented, to achieve an effective rating. For example, the Department would need to develop and implement an effective quality control review process to help ensure adequate supporting documentation is completed prior to its disposal or reuse for digital media sanitization.

Finding 3. The Department's Data Protection and Privacy Program Needs Improvement

We found that for the Data Protection and Privacy metric domain, the Department was at the Consistently Implemented level for one metric question and the Defined level for one metric question. We determined the Department and FSA's controls needed improvement for documenting privacy impact analyses and system of records and notices and documenting the sanitization of digital media.

Documentation Not Complete Supporting Sanitization of Digital Media

According to NIST SP 800-53, Revision 5, Information System Owners are required to sanitize system media prior to disposal, release out of organizational control, or release for reuse using sanitization techniques and procedures detailed in NIST SP 800-88, Revision 1: Media Sanitization guidelines. In accordance with NIST SP 800-88, once sanitization is complete, the forensic analyst examines the drive on a sector-by-sector basis to view and ensure each physical sector has the correct wipe code values, if deemed necessary. Sanitization mechanisms used must provide the strength and integrity commensurate with the security category or classification of the information.

The Department was unable to provide sufficient documentation to support digital media sanitization prior to its disposal or reuse. According to Department officials, when an employee or contractor is terminated, an offboarding request is submitted via ServiceNow.[7] As part of the sanitization process, decommissioned network hardware is erased, reset to its factory settings, then manually accessed to verify the destruction of Department-specific information. Government furnished equipment is sanitized using a "clear sanitization"[8] process. Hard drives or tape drives are degaussed to remove all data, and then physically destroyed or securely disposed of with Certificates of Destruction provided to the Department.

The Department provided a list of departed or soon to be departing individuals from two select systems. We judgmentally selected a sample of 5 individuals from 1 system, and 17 from another system that were offboarded, or soon to be offboarded, between October 1, 2021, and February 2022. We requested evidence showing that proper documentation of clear sanitizing for all digital media assigned to the 22 judgmentally selected individuals. However, no evidence was provided for all 22 individuals showing that a "Certificate of Sanitization," or other alternate electronic ServiceNow record showing the sanitization, was completed. The Department provided screenshots displaying BitLocker logs and Roll-off forms[9] with no additional details. The completed

[7] The ServiceNow Service Automation Government Cloud Suite is a suite of natively integrated applications designed to support IT service automation, resource management and shared support services. The ServiceNow platform includes easy-to-use, point-and-click customization tools to help customers create solutions for unique business requirements.

[8] Clear Sanitization process, factory resets the government furnished equipment, overwrites all user-addressable storage, and recreates the filesystem and OS using a verified image.

[9] The Roll-off form is a generic form that did not provide evidence of media sanitization, but rather served as a promise to return the equipment and did not have a tracking mechanism in place to evidence sanitization had occurred.

forms are submitted by the transitioning user on the date of transition. We found that the Department did not provide sufficient documentation to support that it is consistently implementing its digital media sanitization policies and processes prior to disposal or reuse of media.

For organizations to have appropriate controls on the information they are responsible for safeguarding, they must properly safeguard used media. If not handled properly, release of these media could lead to an occurrence of unauthorized disclosure of information, particularly PII. This could lead to data leakage, exposure, and serious damage to the Department's reputation.

We reported similar conditions in our FY 2021 FISMA audit.

Other Report Findings Impacting Data Protection and Privacy

In the Respond security function, under the Incident Response metric domain of this report, we found weaknesses in the Department's data loss prevention capabilities that allowed PII to be unblocked during transmission.

Recommendations

We recommend that the Chief Information Officer require the Senior Agency Official for Privacy to—

3.1 Implement monitoring and oversight controls to ensure media sanitization policies and processes are in place and document evidence of the disposal or reuse of all used digital media.

3.2 Update digital media sanitization policies and processes to include all requirements outlined in Federal regulations.

Department Comments

The Department agreed with Recommendations 3.1, 3.2 and committed to address these recommendations by September 30, 2022.

OIG Response

OIG will review the proposed corrective action plans to determine whether the actions will address the finding and recommendations and, if so, will validate those actions during our FY 2023 FISMA assessment.

Metric Domain 6—Security Training

Security awareness training is a formal process for educating employees and contractors about IT security pertaining to the confidentiality, integrity, and availability of information. This includes ensuring that all people involved in using and managing IT

understand their roles and responsibilities related to the organizational mission; understand the organization's IT security policy, procedures, and practices; and have adequate knowledge of the various management, operational, and technical controls required to protect the IT resources for which they are responsible. For example, we judgmentally selected a small sample of new user accounts and verified that security training was completed.

We determined that the Department's security training program was consistent with the Managed & Measurable Implemented level (level 4) of the maturity model, which is considered effective.

Progress Made in FY 2022

We found the Department took several actions to improve its security training posture, as shown in Table 9.

Table 9. Security Training Actions Taken

Areas Improved	Actions Taken
Policies, Procedures, and Standards	Established and updated its cybersecurity policy framework in alignment with Executive Order 14028 and NIST SP 800-53 Version 5. Established the Information Technology System Awareness and Training Standard (1/31/2022); the Information Technology Program Management (1/31/2022). OCIO's Information Assurance Services established an Information Technology Cybersecurity Awareness and Training Program Two-Year Tactical Plan for FYs 2022–2023, and FY 2022 Simulated Phishing Exercise Plan.

Areas Improved	Actions Taken
Enterprise-Wide Training Strategy	The Department implemented new Skillsoft online learning platform to enhance existing courses and curriculum offered through FedTalent. It also used Mediasite recordings to increase outreach to users that prefer to complete training outside of the Department's Learning Management System for IT Security Role Based Training and Training for Employees with Significant Security Responsibilities. The new FY 2022 Cybersecurity and Privacy Awareness Course 1 enabled learners to satisfy course requirements using two methods. The first method was to successfully complete a test out feature which used a series of difficult questions to assess the users existing knowledge of topic areas contained within the course. The second method was to complete the course curriculum and respond to interactive scenarios. Role-based training content was developed and provided by the Department and made available in FedTalent as courses, ebooks, videos, and other resources (i.e., web-based training within the Department learning management systems, OCIO Mediasite recorded training, and training provided through Federal Virtual Training Environment). The Department continued to address workforce knowledge, skills, and abilities gaps through training or hiring of additional staff or contractors. To assist employees and contractors with completion of required training, the Department continues to research and develop new opportunities at no-cost training available through participation in the annual Cybersecurity Symposium, OCIO/IAS Quarterly Risk Management Workshops, and FSA Information Systems Security Officer Working Group meetings.

The Department achieved the Managed and Measurable level (level 4) of security in the core metric question for the Security Training metric domain.

We did not identify new findings for the Security Training metric domain for FY 2022. All corrective action plans for recommendations from previously reported findings were implemented at the close of our inspection fieldwork.

Recommendations

There are no new recommendations for the Security Training metric domain.

Detect

The Detect security function is comprised of the information security continuous monitoring (ISCM) metric domain. Based on our evaluation of the Department's ISCM program, we determined the Detect security function was consistent with the Managed and Measurable level (level 4) of the maturity model, which is considered effective. The Department continued to develop and strengthen its ISCM program. However, we noted

that improvements were needed to its processes for collecting and analyzing ISCM performance measures and reporting findings.

Metric Domain 7—Information Security Continuous Monitoring

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

We determined that the Department's ISCM program was consistent with the Managed and Measurable level (level 4) of the maturity model, which is considered effective.

Progress Made in FY 2022

We found the Department took several actions to improve its information security continuous management posture, as shown in Table 10

Table 10. Information Security Continuous Monitoring Actions Taken

Areas Improved	Actions Taken
Policies, Procedures, and Standards	Established and updated its cybersecurity policy framework in alignment with Executive Order 14028 and NIST SP 800-53, Version 5. The Department established an Information Technology System Security Assessment and Authorization Standard (1/ 31/2022). Updated ISCM policies and standards to reflect and support the ISCM Roadmap, ongoing assessment and authorization, vulnerability management standards, the ISCM Current State Assessment Policy.
Enterprise-Wide ISCM Function	Monitors and maintains ongoing authorizations of information systems, including the maintenance of system security plans. The Department confirmed a security assessment team works with OCIO to implement the ongoing security assessment program to replace the older static-point-in-time assessment model of assessment and authorization. The goal is to transitions all systems to the ongoing security assessment program.
Collecting and analyzing ISCM performance measures.	Monitors, and analyses qualitative and quantitative performance measures on the ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting defined in the ISCM Roadmap. Established a security assessment report and system security plans issuance process. Implemented the Continuous Diagnostic Mitigation Maturity Model process. Established a process to update the cybersecurity framework risk daily to reflect each system cybersecurity posture score.

The OIG made prior recommendations in FY 2019 and FY 2020 that the Department automate its capabilities for monitoring the security controls effectiveness and overall implementation of the ISCM Roadmap. We also recommended the Department establish oversight controls to review, monitor and verify progress of the ISCM strategy, as well as the annual reviews of all Departmental cyber security policies, to reflect the current environment.

We found the department uses the Cybersecurity Scorecard to monitor and analyze performance measures on the effectiveness of its ISCM policies and strategy. We reviewed the Department's ISCM strategy and supporting ISCM policies and determined ISCM policies support the ISCM strategy and address ISCM requirements at each organizational tier.

The Department achieved the Managed and Measurable level (level 4) of security in both core metric questions for the ISCM metric domain.

We did not identify new findings for the Information Security Continuous Monitoring metric domain for FY 2022. All corrective action plans for recommendations from previously reported findings were implemented at the close of our inspection fieldwork.

Recommendations

There are no new recommendations for the ISCM metric domain.

Respond

The Respond security function is comprised of the Incident Response metric domain. Based on our evaluation, we determined the Respond security function was at the Managed and Measurable level (level 4) of the maturity model, which is considered effective. We found that the Department continued to develop and strengthen its incident response program. However, we noted that improvements are needed in the Department's program. For instance, we found that the data loss prevention policy and process should be updated to incorporate new technologies or solutions used for the transmission of PII.

Metric Domain 8—Incident Response

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

We found that for the Incident Response metric domain, the Department was at the Managed and Measurable level (level 4) for one core metric question and the Consistently Implemented level (level 3) for one core metric question, and an overall Managed and Measurable level (level 4), which is effective.

Progress Made in FY 2022

We found the Department took several actions to improve its incident response risk management posture, as shown in Table 11.

Table 11. Incident Response Risk Management Actions Taken

Areas Improved	Actions Taken
Policies, Procedures and Processes	Established and updated its cybersecurity policy framework in alignment with Executive Order 14028 and SP NIST 800-53, Version 5. Established the Information Technology Incident Response Standard (1/31/2022). The Department updated its policy, guidance, standards, checklist including the Department Incident Reporting Guidelines and the Incident Response Plan. The Department continues to review and evolve its processes to further improve incident response time, effectiveness, and consistency.
Roles and Responsibilities	Established an across-the-board effort to review internal documentation, update captured metadata in ticketing systems, as well as data ingestion and reporting improvements. Coordinates both scheduled and ad-hoc meetings between the response teams to ensure appropriate delegation of responsibilities and rapid dissemination of important information is performed daily. This includes the Cyber Fusion Meeting, that allows members of the various teams to collaborate in a free-form setting without a fixed agenda.
Incident Response Tools and Technologies	Implemented an enhanced ticketing quality assurance procedure, updated configurations for existing tools, and new tool deployments.

Finding 4. The Department's Incident Response Program Needs Improvement

For the Incident Response domain, although rated at the Managed and Measurable level, we found one area where the Department and FSA can further enhance their controls for their compliance with Federal and Departmental reporting guidelines.

Compliance with Federal and Departmental Reporting Guidelines

The United States Computer Emergency Readiness Team Federal Incident Notification Guidelines requires agencies to report security incidents along with the required data elements within one hour of being identified. The Department's Education Security Operations Center relies on RSA Archer Internal Cybersecurity Investigations Ticketing System as its incident response ticketing system. As part of the ticketing system process, quality control steps are performed on all daily tickets to ensure that all required information corresponds exactly with the Federal review audit.

Our testing found that the Department didn't always comply with the United States Computer Emergency Readiness Team notification guidelines, timeframes, and communications of relevant incidents to the OIG. We obtained the Department's computer security incident report for the identified 16,516 incidents. Out of the 16,516 incidents, 259 were determined to be incidents by the Education Security Operations Center Coordinator. For the 259 incidents, we reviewed those incidents that were created between October 1, 2021, and May 20, 2022, which accounted for 99 relevant incidents. Out of the 99 incidents, 11 incidents did not include common attack vectors taxonomy, 8 incidents did not include incident category, 2 incidents were not reported to United States Computer Emergency Readiness Team within the required timeframe, and 1 incident was not immediately reported to OIG or law enforcement. We also noted inconsistencies with reporting. For instance, 6 out of 99 incidents that should have been reported to OIG were not.

According to the United States Computer Emergency Readiness Team Federal Incident Notification Guidelines, agencies must report information security incidents where the confidentiality, integrity, or availability of a Federal information system of a civilian Executive Branch agency is potentially compromised, to the Cybersecurity and Infrastructure Security Agency/ United States Computer Emergency Readiness Team with the required data elements, as well as any other available information, within one hour of being identified by the agency's top-level Computer Security Incident Response Team, Security Operations Center, or information technology department (which, for the Department, is the Education Security Operations Center Coordinator). This is consistent with the Department's incident notification guidelines that state all incidents are to be reported to United States Computer Emergency Readiness Team and other relevant parties, such as OIG, within one hour.

Enhance Data Loss Prevention Strategy

Consistent with its policy, the Department has demonstrated that its data loss prevention tools protect against the outbound transmission of PII and sensitive PII within the Microsoft Office 365 Outlook environment. This includes string matches containing social security numbers and credit card numbers. However, with the emerging technology of new communication platforms, the Department will need to

ensure that it continues to enhance its data loss protection policy to meet the security needs of emerging communication platforms.

The Department's standard for safeguarding PII and Sensitive PII, "Standard PR.DS: PII Data Loss Prevention—Microsoft Office 365" requires that the data loss prevention settings must identify social security and credit card numbers contained within outgoing email traffic (both Departmental user and non-Departmental user) as PII. According to NIST SP 800-137, ISCM for Federal Information Systems and Organizations, an effective data loss prevention strategy includes tools to monitor data at rest, in use, and in transit. In addition, the effective use of data loss prevention technologies can assist organizations in automating the implementation, assessment, and continuous monitoring of several NIST SP 800-53 security controls.

During our fieldwork, we identified a non-email communication platform that had recently integrated a data loss prevention strategy into its processes. We tested the platform and found it did not have data loss prevention defense capabilities. We are reporting this information to the Department to ensure they are aware and to assist them in assessing risk and possibly developing compensating controls for the communication platform we tested.

Without effective data loss prevention solution, a malicious user or insider threat actor could circumvent the data loss prevention defenses without being detected. As a result, public confidence in the Department's abilities to protect personal financial information, such as social security numbers and credit card numbers, could decrease and cause serious damage to the Department's reputation.

Recommendation:

We recommend that the Chief Information Officer require OCIO to—

4.1 Establish oversight controls to ensure that the Department follows United States Computer Emergency Readiness Team required notification guidelines, timeframes, and communicates the relevant incidents to the OIG.

Department Comments

The Department agreed with Recommendation 4.1 and committed to address this recommendation by September 30, 2022.

OIG Response

OIG will review the proposed corrective action plan to determine whether the actions will address the finding and recommendations and, if so, will validate those actions during our FY 2023 FISMA assessment.

Recover

The Recover security function is comprised of the Contingency Planning metric domain. Based on our evaluation of the Department's contingency planning program, we determined the Recover security function was at the Managed & Measurable level (level 4) of the maturity model, which is considered effective.

Metric Domain 9—Contingency Planning

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

Progress Made in FY 2022

We found the Department took several actions to improve its contingency planning posture, as shown in Table 12.

Table 12. Contingency Planning Actions Taken

Areas Improved	Actions Taken
Policies and Procedures	Established and updated its cybersecurity policy framework in alignment with Executive Order 14028 and NIST SP 800-53 Version 5. Established the Information Technology Contingency Planning Standard (1/31/2022). Added the Business Continuity Plan Template Version 1.0 (2/1/2022). Established the System Security Plan Review Checklist (2/11/2022). Established the Standard ID.GOV Required Authorization Documentation (9/1/2021). Established the Information System Contingency Planning Guidance to reflect changes in requirements for Contingency Plans, Contingency Plan Testing, Disaster Recovery Plans, Disaster Recovery Plan Testing, and Business Impact Analysis. Established the Tabletop Exercise Standard Operating Procedure, Version 2.0 (8/30/2021). Established the Department of Education Continuity Plan (January 2022). Established the Information System Contingency Plan Guidance (2/1/2022). Established the Business Impact Analysis template (2/25/2022). Established the Disaster Recovery Plan Template, Version 1.5 (2/1/2022). Established the Contingency Plan and Contingency Plan Test Template Version 1.2 (2/1/2022).

Areas Improved	Actions Taken
Business Impact Analysis and Contingency Plans and Testing	Made enhancements to tabletop exercises to include cyber security attacks. Updated requirements for contingency planning documents for cloud service provider systems. Made enhancements Cyber Security Risk Scorecard and Power BI reporting. Developed the daily Cyber Security Assessment and Management discrepancies report and the daily security documentation report (generated from Power BI) to capture the status of required system documents. Developing the Daily Score Card and Daily Cyber Security Assessment and Management Discrepancies Report, as well as the Daily Plan of Action and Milestones Report (through use of the Power BI Tool) to help the system stakeholders to identify, analyze and track assessment and authorization compliance.

The Department achieved the Managed and Measurable level of security in all core metric questions for the Contingency Planning metric domain.

We did not identify new findings for the Contingency Planning metric domain for FY 2022. All corrective action plans for recommendations from previously reported findings were implemented at the close of our inspection fieldwork.

Recommendations

There are no new recommendations for the Contingency Planning metric domain.

Other Matters. Cybersecurity Standards

A memorandum was signed by the Department's Chief Information Security Officer on February 2, 2022, to establish an enterprise-wide information security program as part of the initiative to safeguard the confidentiality, integrity, and availability of its information and systems. The OCIO Information Assurance Services division also issued new ED cybersecurity standards to support the ongoing implementation of Executive Order 14028, Improving the Nation's Cybersecurity. The standards are organized using the 20 control families contained within the NIST SP 800-53, Revision 5, issued in September 2020.

Effective immediately, all new Department information systems and existing systems undergoing major modifications, to the extent modifications intersect with the updated requirements, are required to comply with the security and privacy controls requirements contained within the new Executive Order 14028 supportive standards. All existing information systems must transition from the legacy standards to the new Executive Order 14028 supportive standards within three months from the date of the memorandum.

For FY 2022, the new Departmental cybersecurity standards were reviewed and used as criteria within the scope of our fieldwork to support our findings and conclusions, as applicable within the scope of our inspection.

Appendix A. Scope and Methodology

Our objective was to assess the Department's progress at improving the maturity of its security program and practices as required by Federal information security requirements. We started our fieldwork on February 15, 2022, and ended on May 31, 2022. For FY 2022, the OIG FISMA metrics require the OIG to evaluate 20 core metrics. The 20-core metrics are organized around the 5 information security functions outlined in NIST's Framework for Improving Critical Infrastructure Cybersecurity: Identify, Protect, Detect, Respond, and Recover.

To answer the objective, we obtained an understanding of the Department's Cybersecurity processes and procedures and conducted inspection work in the 9 metric domains within the 5 Security functions associated with the 20 core metric areas: (1) Risk Management, (2) Supply Chain Risk Management, (3) Configuration Management, (4) Identity and Access Management, (5) Data Protection and Privacy, (6) Security Training, (7) Information Security Continuous Monitoring, (8) Incident Response, and (9) Contingency Planning.

We obtained and reviewed the necessary information to obtain an understanding of the Departments processes and procedures. Specifically, we

- obtained written responses from Department and FSA officials and contractor personnel, with knowledge of system security and application management, operational, and technical controls;
- reviewed applicable information security regulations, standards, and guidance;
- gained an understanding of IT security controls by reviewing policies, procedures, and practices that the Department implemented at the enterprise and system levels;
- obtained direct access to the Federal Risk and Authorization Management Program cloud service provider security packages for select systems; and
- assessed the Department's enterprise and system-level security controls.

We conducted testing to verify processes and procedures were in place. Specifically, we

- reviewed corrective action plans identified starting from July 1, 2021, through April 31, 2022;
- tested management, operational, and technical controls based on NIST standards and Department guidance;

- performed system-level testing for the Risk Management, Configuration Management, Data Protection and Privacy, and Contingency Planning metric domains;
- conducted vulnerability scans for two of three FSA and Department systems;[10]
- identified users for compliance with the security training;
- observed the 2022 Department's and FSA's disaster recovery tabletop exercises and test, conducted in a virtual setting;
- reviewed computer security incidents that were reported from October 1, 2021, and May 20, 2022;
- tested websites for encryption protocols;
- tested and review the Department's virtual private network protocols and solution;
- performed vulnerability assessment testing on the two selected systems;
- verified security settings for Department data protection; and
- participated in the Department Cybersecurity Risk Management workshops.

Sampling Methodology

As of December 22, 2021, an inventory of 151 systems that were FISMA-reportable and classified as operational were identified. Of the 151 FISMA-reportable systems, 115 were classified as moderate-impact systems, and 36 as low-impact systems.

During FISMA FY 2022, the OIG focused on the inspection and testing of Department systems hosted in a cloud-based or cloud-dependent environment. The Department's Enterprise Cloud strategy (2021–2023) has established objectives that align with Federal Cloud Computing Strategy objectives: Efficiency, Agility, and Innovation. Benefits of the objectives include the following:

- Increase the Department's effectiveness to search and combine critical information from different systems across the enterprise.
- Leverage efforts such as FedRAMP to standardize and streamline the Department's ability to share IT capabilities across the enterprise to support the continual reauthorization and assessment of authorization processes and implementation of continuous monitoring.

[10] The specific results of our testing were provided to the Department and FSA for review and action.

- Move to standardize and simplify ICAM.

As a result, we selected a non-statistical sample of 3 out of 42 systems, which represented approximately 7 percent of all systems in their relevant population. All three selected systems had a Federal Information Processing Standards Publication 199 impact level of either high or moderate.[11]

In making our selection, we considered risk-based characteristics such as system classifications (high or moderate), systems classified as high-value assets, systems classified as cloud service providers providing key business services, systems classified as cloud dependent, new systems, and systems containing PII.

Table 12 lists the judgmentally selected systems, the system's principal office, and the Federal Information Processing Standards Publication 199 potential impact level.

Table 12. OIG Judgmentally Selected Systems

Number	System Name	Principal Office	Impact Level
1	Department—ServiceNow Service Automation Government Cloud Suite	OCIO	Moderate
2	Education Security Tracking and Reporting System	OFO	Moderate
3	Enterprise Data Management and Analytics Platform Services	FSA	Moderate

Testing of these systems helped us ascertain the security control aspects relating to Risk Management, Configuration Management, Data Protection and Privacy, and Contingency Planning metrics.[12] In addition, two of these systems were the focus of our system vulnerability assessment and testing.

[11] Federal Information Processing Standards Publication 199 defines 3 levels of potential impact on organizations should there be a breach of security (that is, a loss of confidentiality, integrity, or availability) as low, moderate, or high.

[12] Because we did not select a statistical random sample, the results of our analysis cannot be projected across the entire inventory of Department IT systems.

In addition to the sample of 3 systems, we also used sampling to test certain aspects in the areas of Configuration Management, Incident Response, Security Training, and Identity and Access Management.

- For Configuration Management, we tested all 640 Departmental websites for encryption protocols; inventory counts; and obsolete operating systems, applications, and databases.[13]
- For Data Protection and Privacy, we judgmentally sampled the Department's digital media sanitization processes for 35 out 920 employees and contractors with access to 2 of 3 selected systems subject to offboarding between October 1, 2021, and April 30, 2022.
- For Security Training, we tested a judgmental sample of 6 out of 17,601 new user accounts created from July 1, 2021, to April 30, 2022.
- For Incident Response, we tested 259 out of 16,516 security events that occurred between October 1, 2021, and February 2022 that were deemed IT incidents.

Where we relied on judgmental sampling and the inspector's judgment, we did not project the results from the above samples.

Use of Computer-Processed Data

For this inspection, we reviewed the security controls and configuration settings for the in-scope systems and applications externally hosted in a cloud environment. We used computer-processed data for the Configuration Management, Identity and Access Management, Security Training, Data Protection and Privacy, and Incident Response metric domains to support the findings summarized in this report. These data were provided by the Department through self-reporting, generated through a system where inspectors did not have rights to access the system, or obtained directly by the inspectors via privileged access granted by the Department. We performed assessments of the computer-processed data to determine whether the data were reliable for the purpose of our inspection. To determine the extent of testing required for the assessment of the data's reliability, we 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 were verified to source data and tested for accuracy according to relevant system controls until enough information was available to make a reliability determination. Finally, inspectors had direct access to the Department's security information repositories to perform independent verification of evidence provided by

[13] The website inventory was also used for testing in the Risk Management metric section.

the Department. We determined data provided by the Department was reliable for the purpose of our inspection.

Compliance with Standards

We prepared this inspection in alignment with OIG's quality control standards and the Council of Inspectors General for Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* (Blue Book), which require that we conduct our work with integrity, objectivity, and independence. We believe that the information obtained provides a reasonable basis for the conclusions and recommendations contained in this report.

Appendix B. Status of Prior Year Recommendations

As part of this year's FISMA inspection, we followed up on the status of prior year recommendations that were closed prior to the end of our fieldwork.[14] If recommendations were implemented and FY 2022 testing identified no findings, OIG closed the recommendations. If recommendations were not implemented at all or were insufficient, we repeated the recommendations from prior years.

Based on our testing of the 77 recommendations from our FY 2019 to FY 2021 reports, we determined that 20 remained open:

- 1 out of 37 remained open from FY 2019,
- 9 out of 24 remained open from FY 2020, and
- 10 out of 16 remained open from FY 2021.

The tables below show repeat and open recommendations from FY 2019 through FY 2021. During FISMA FY 2020, the OIG focused entirely on the testing Departmental systems part of the PIVOT environment. For the FISMA FY 2021, OIG focused on systems managed by the FSA.

Table 13. FY 2019, OIG Audit Control Number A11T0002

Number	Recommendation	Status	PCD/ACD	OIG Determination
2.4	We recommend that the Deputy Secretary require OCIO to ensure that 51 websites are routed through a trusted internet connection or managed trusted internet protocol service.	Open	03/31/2023	Open

[14] We performed additional testing to assess the Department's progress related to several open prior year findings, including Masking of PII, Strong User Authentication Mechanisms, Websites Configured with Warning Banners, and websites not configured to use HTTPS to encrypt traffic. The results, if any, will be discussed with the Department but will remain open after the end of our fieldwork date. We will follow up in future FISMA audits to confirm whether the corrective actions are implemented.

Table 14. FY 2020, OIG Audit Control Number A11U0001

Number	Recommendation	Status	PCD/ACD	OIG Determination
2.2	We recommend that the Deputy Secretary and Chief Operating Officer require that OCIO and FSA migrate to Transport Layer Security 1.2 or higher as the only connection for all Department connections.	Open	12/30/2021	Repeat
2.3	We recommend that the Chief Information Officer require the Department to enhance implementation controls to prioritize and apply the most up-to-date and timely software patches and security updates to the identified systems and information technology solutions.	Open	09/30/2021	Repeat
2.6	We recommend that the Chief Information Officer require the Department to correct or mitigate the vulnerabilities identified during the security assessment, in accordance with the severity level of each vulnerability identified.	Closed	09/30/2021	Repeat
3.1	We recommend that the Chief Information Officer require the Department to establish oversight controls to ensure the Department's password, terminations, and deactivation policies are enforced accordingly.	Open	09/30/2021	Repeat
3.2	We recommend that the Chief Information Officer require the Department to enforce the mandate for all websites to display warning banners when user's login to Departmental resources and establish additional procedures and monitoring processes to ensure that banners include the approved warning language. (Incorporates a Repeat Recommendation)	Reopened	6/30/2021	Repeat
7.2	We recommend that the Chief Information Officer require the Department to develop and implement oversight controls to ensure that incidents are consistently submitted to US-CERT and the OIG within the required timeframes, are consistently categorized, and include the correct vector elements as required.	Open	09/30/2021	Repeat

Number	Recommendation	Status	PCD/ACD	OIG Determination
7.4	We recommend that the Chief Information Officer require the Department to develop and implement testing procedures and enhance current policies and processes to ensure that the DLP solution works as intended for the blocking of sensitive information transmission. (Incorporates a Repeat Recommendation)	Reopened	3/2/2021	Repeat
1.4	We recommend that the Chief Information Officer require the Department to establish and automate procedures to ensure all Department-wide IT inventories are accurate, complete, and periodically tested for accuracy. Include steps to establish that all IT contracts are reviewed and verified for applicable privacy, security, and access provisions. (Incorporates a Repeat Recommendation)	Open	9/30/2022	Open
2.4	We recommend that the Chief Information Officer require the Department to Establish stronger monitoring controls to enforce the management of unsupported system components and track and discontinue the use of unsupported operating systems, databases, and applications. (Incorporates a Repeat Recommendation)	Open	9/30/2022	Open

Table 15. FY 2021, OIG Audit Control Number A21IT0023

Number	Recommendation	Status	PCD/ACD	OIG Determination
3.1	We recommend that the Chief Information Officer require OCIO to—Take steps to assure obsolete solutions and encryption protocols are either updated, removed, or replaced.	Open	4/8/2022	Repeat
3.2	We recommend that the Chief Information Officer require OCIO to—Implement additional measures for patches to be applied in a timely manner based on a priority basis.	Open	4/8/2022	Repeat

Number	Recommendation	Status	PCD/ACD	OIG Determination
5.1	We recommend that the Chief Information Officer require the SAOP to—Implement monitoring and oversight controls that ensure employees and contractors are adhering to current media sanitization policies and are correctly documenting and validating the disposal or reuse of used digital media. In addition, provide adequate evidence showing the proper documentation and validating of clear sanitizing for all digital media assigned to the sampled 10 offboarded employees or contractors. Lastly, ensure the digital media sanitization policies and processes are completed, as appropriate, to capture all requirements dictated by Federal regulations.	Open	12/23/2021	Repeat
3.3	We recommend that the Chief Information Officer require OCIO to—Ensure all Department websites are configured to mask PII when used as an identifier.	Open	6/30/2022	Open
3.4	We recommend that the Chief Information Officer require OCIO to—Enforce secure connections as required by OMB M-15-13 for all existing websites and services.	Open	6/30/2022	Open
4.1	We recommend that the Chief Information Officer require OCIO to—Fully implement ICAM Strategy by established milestones to ensure the Department meets full Federal government implementation of ICAM.	Open	6/30/2022	Open
4.4	We recommend that the Chief Information Officer require OCIO to—Enforce a two-factor authentication configuration for all user connections to systems and applications.	Open	6/30/2022	Open
4.5	We recommend that the Chief Information Officer require OCIO to—Perform and evidence regularly scheduled reviews of system user accounts (both privileged and nonprivileged) to recertify and maintain each Department system's validity.	Open	6/30/2022	Open
4.6	We recommend that the Chief Information Officer require OCIO to—Remove terminated users' access to Department resources timely in accordance with Departmental policy.	Open	6/30/2022	Open

Number	Recommendation	Status	PCD/ACD	OIG Determination
4.7	We recommend that the Chief Information Officer require OCIO to—Identify and enforce all websites to display warning banners when users login to Departmental resources.	Open	6/30/2022	Open

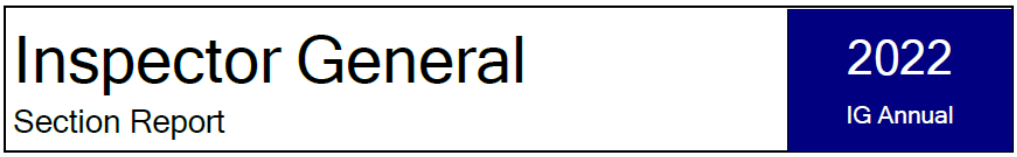
Appendix C. Domain Maturity Ratings

Table 16. Domain Maturity Ratings FY 2021 and FY 2022

Security Function	Metric Domain	FY 2021 Domain Maturity Rating	FY 2022 Domain Maturity Rating
Identify	Risk Management	Consistently Implemented	Consistently Implemented
Identify	Supply Chain Risk Management	Defined	Consistently Implemented
Protect	Configuration Management	Consistently Implemented	Managed and Measurable
Protect	Identity and Access Management	Defined	Consistently Implemented
Protect	Data Protection and Privacy	Defined	Consistently Implemented
Protect	Security Training	Consistently Implemented	Managed and Measurable
Detect	Information Security Continuous Monitoring	Consistently Implemented	Managed and Measurable
Respond	Incident Response	Consistently Implemented	Managed and Measurable
Recover	Contingency Planning	Consistently Implemented	Managed and Measurable

Appendix D. CyberScope 2022 IG FISMA Metrics

For Official Use Only



Department of Education

For Official Use Only

Function 0: Overall

0.1. Please provide an overall IG self-assessment rating (Effective/Not Effective)

Effective

0.2. Please provide an overall assessment of the agency's information security program. The narrative should include a description of the assessment scope, a summary on why the information security program was deemed effective/ineffective and any recommendations on next steps. Please note that OMB will include this information in the publicly available Annual FISMA Report to Congress to provide additional context for the Inspector General's effectiveness rating of the agency's information security program. OMB may modify the response to conform with the grammatical and narrative structure of the Annual Report.

Our objective was to assess the U.S. Department of Education's (Department) progress at improving the maturity of its security program and practices as required by the Federal Information Security Modernization Act of 2014. In the fiscal year 2022, our inspection focused on 20 core metrics within the 5 security functions and the 9 associated metric domains for cybersecurity management. To answer the objective, we evaluated the Department's security program using the 20 core Inspector General Reporting Metrics that were published for the fiscal year 2022 and issued by the Office of Management and Budget. We determined the Department's programs were consent with Level 3 - Consistently Implemented, which is considered not effective for four domains Risk Management, Supply Chain Risk Management, Identity and Access Management, and Data Protection and Privacy. Level 4- Managed and Measurable which is considered effective for five domains Configuration Management, Security Training, Information System Continuous Monitoring, Incident Response, and Contingency Planning.

Function 1A: Identify - Risk Management

1. To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third-party systems), and system interconnections? (NIST SP 800-53, Rev. 5: CA-3 and PM-5; NIST Cybersecurity Framework (CSF): ID.AM-1 - 4; FY 2022 CIO FISMA Metrics: 1.1-1.1.5, 1.3; OMB A-130, NIST SP 800-37, Rev. 2: Task P-18; NIST 800-207, Section 7.3; EO 14028, Section 3; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B and D (5); CISA Cybersecurity & Incident Response Playbooks)

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED- OIG/I22IT0066 (FISMA Report) The Department's Risk Management Program Needs Improvement

2. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE and Bring Your Own Device (BYOD) mobile devices) connected to the organization's network with

Function 1A: Identify - Risk Management	
	the detailed information necessary for tracking and reporting ? (NIST SP 800-53, Rev. 5: CA-7 and CM-8; NIST SP 800-137; NIST IR 8011; NIST 800-207, 7.3.2; Federal Enterprise Architecture (FEA) Framework, v2; FY 2022 CIO FISMA Metrics: 1.2-1.2.3; CSF: ID.AM-1, ID.AM-5; NIST SP 800-37, Rev. 2: Task P-10 and P-16; NIST 800-207, Section 7.3; EO 14028, Section 3; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8: Control 1) Consistently Implemented (Level 3) *Comments*: Consistently Implemented (Level 3) - ED- OIG/I22IT0066 (FISMA Report) The Department's Risk Management Program Needs Improvement
3.	To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets (including GFE and Bring Your Own Device (BYOD) mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting ? (NIST SP 800-53, Rev. 5: CA-7, CM-8, CM-10, and CM-11; NIST SP 800-137; NIST IR 8011; FEA Framework, v2; FY 2022 CIO FISMA Metrics: 1.3 and 4.0; OMB M-21-30; EO 14028, Section 4; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B; CSF: ID.AM-2; NIST SP 800- 37, Rev. 2: Task P-10 and P-16; NIST 800-207, Section 7.3; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8: Control 2) Consistently Implemented (Level 3) *Comments*: Consistently Implemented (Level 3) - ED- OIG/I22IT0066 (FISMA Report) The Department's Risk Management Program Needs Improvement
4.	To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets (NIST SP 800-53 Rev. 4: RA-2, PM-7, and PM-11; NIST SP 800-60; NIST SP 800-37 (Rev. 2); CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2022 CIO FISMA Metrics: 1.1; OMB M-19-03; NIST SP 800-37, Rev. 2: Task C-2, C-3, P-12, P-13, S-1 - S-3)?
5.	To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels? (NIST SP 800-39; NIST SP 800-53, Rev. 5: RA-3 and PM-9; NIST IR 8286; CSF: ID RM-1 - ID.RM-3; OMB A-123; OMB M-16-17; OMB M-17-25; NIST SP 800-37 (Rev. 2): Tasks P2, P-3, P-14, R-2, and R-3) Managed and Measurable (Level 4)
6.	To what extent does the organization utilize an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain (Federal Information Technology Acquisition Reform Act (FITARA), NIST SP 800-39; NIST SP 800-160; NIST SP 800-37 (Rev. 2) Task P-16; OMB M-19-03; OMB M-15-14, FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-161; NIST SP 800-163, Rev. 1 CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?

For Official Use Only

Function 1A: Identify - Risk Management

7. To what extent have roles and responsibilities of internal and external stakeholders involved in cyber security risk management processes been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1, 2.3.2, and Appendix D; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; NISTIR 8286, Section 3.1.1, OMB A-123;; NIST SP 800-37 (Rev. 2) Section 2.8 and Task P-1; OMB M-19-03)?

8. To what extent has the organization ensured that plans of action and milestones (POA&Ms) are utilized for effectively mitigating security weaknesses (NIST SP 800-53 Rev. 4: CA-5; NIST SP 800-37 (Rev. 2) Task A-6, R-3; OMB M-19-03, CSF v1.1, ID.RA-6)?

9. To what extent does the organization ensure that information about cyber security risks is communicated in a timely manner to all necessary internal and external stakeholders (OMB A-123; OMB Circular A-11; Green Book (Principles #9, #14 and #15); OMB M-19-03; CSF: Section 3.3; NIST SP 800-37 (Rev. 2) Task M-5; SECURE Technology Act: s. 1326, NISTIR 8286)?

10. To what extent does the organization utilize 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? (NIST SP 800-39; OMB A-123; NIST IR 8286; CISA Zero Trust Maturity Model, Pillars 2-4, NIST 800-207, Tenets 5 and 7; OMB M-22-09, Federal Zero Trust Strategy, Security Orchestration, Automation, and Response)

Managed and Measurable (Level 4)

11.1. Please provide the assessed maturity level for the agency's Identify - Risk Management program.

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED- OIG/I22IT0066 (FISMA Report) The Department's Risk Management Program Needs Improvement

11.2. Provide any additional information on the effectiveness (positive or negative) of the organization's Risk Management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?

Function 1B: Identify - Supply Chain Risk Management

12. To what extent does the organization utilize supply chain risk management policies and procedures to manage SCRM activities at all organizational tiers (NIST SP 800-37 Rev. 2, Section 2.8, NIST 800-53, SR-1, NIST CSF v1.1, ID.SC-1, NIST 800-161)?

13. To what extent does the organization utilize a supply chain risk management plan(s) to ensure the integrity, security, resilience, and quality of services, system components, and systems (OMB A-130, NIST SP 800-37 Rev. 2, Section 2.8, NIST 800-53, SR-2, SR-3; NIST 800-161, section 2.2.4 and Appendix E)?

14. To what extent does the organization ensure that products, system components, systems, and services of external providers are

Function 1B: Identify - Supply Chain Risk Management

consistent with the organization's cybersecurity and supply chain requirements? (The Federal Acquisition Supply Chain Security Act of 2018, NIST SP 800-53, Rev. 5: SA-4, SR-3, SR-5 and SR-6 (as appropriate); NIST SP 800-152; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4, NIST IR 8276, NIST 800-218, Task PO.1.3; FY 2022 CIO FISMA Metrics: 7.4.2; CIS Top 18 Security Controls v.8: Control 15)

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED- OIG/I22IT0066 (FISMA Report) The Department's Supply Chain Risk Management Program Needs Improvement

15. To what extent does the organization maintain and monitor the provenance and logistical information of the systems and system components it acquires? (NIST SP 800-53 REV. 5: SR-4 and NIST SP 800-161, Provenance (PV) family)?

16.1. Please provide the assessed maturity level for the agency's Identify - Supply Chain Risk Management program.

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED- OIG/I22IT0066 (FISMA Report) The Department's Supply Chain Risk Management Program Needs Improvement

16.2. Please provide the assessed maturity level for the agency's Identify Function.

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED- OIG/I22IT0066 (FISMA Report) The Department's Risk Management and Supply Chain Risk Management Program Needs Improvement

16.3. 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 risk management program effective?

Function 2A: Protect - Configuration Management

17. To what extent have the roles and responsibilities of configuration management stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: CM-1; NIST SP 800-128: Section 2.4)?

18. To what extent does the organization utilize an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems (NIST SP 800-128: Section 2.3.2; NIST SP 800-53 REV. 4: CM-9)?

19. To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related

Function 2A: Protect - Configuration Management	
	components at a level of granularity necessary for tracking and reporting (NIST SP 800-53 REV. 4: CM-2 and CM-8; FY 2022 CIO FISMA Metrics: 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and PR.IP-1)?
20.	To what extent does the organization utilize settings/common secure configurations for its information systems? (NIST SP 800-53, Rev. 5: CM-6, CM-7, and RA-5; NIST SP 800-70, Rev. 4; FY 2022 CIO FISMA Metrics, Section 7, Ground Truth Testing; EO 14028, Section 4, 6, and 7; OMB M-22-09, Federal Zero Trust Strategy, Section D; OMB M - 22-05; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8, Controls 4 and 7; CSF: ID.RA-1 and DE.CM-8) **Managed and Measurable (Level 4)**
21.	To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities? (EO 14028, Sections 3 and 4; NIST SP 800-53, Rev. 5: CM-3, RA-5, SI-2, and SI-3; NIST SP 800-40, Rev. 3; NIST 800-207, section 2.1; CIS Top 18 Security Controls v.8, Controls 4 and 7; FY 2022 CIO FISMA Metrics: Section 8; CSF: ID.RA-1; DHS Binding Operational Directives (BOD) 18-02, 19-02, and 22-01; OMB M-22-09, Federal Zero Trust Strategy, Section D; CISA Cybersecurity Incident and Vulnerability Response Playbooks) **Managed and Measurable (Level 4)**
22.	To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-19-26)?
23.	To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate (NIST SP 800-53 REV. 4: CM-2, CM-3 and CM-4; CSF: PR.IP-3).
24.	To what extent does the organization utilize a vulnerability disclosure policy (VDP) as part of its vulnerability management program for internet-accessible federal systems (OMB M-20-32 and DHS BOD 20-01)?
25.1.	Please provide the assessed maturity level for the agency's Protect - Configuration Management program. **Managed and Measurable (Level 4)**
25.2.	Provide any additional information on the effectiveness (positive or negative) of the organization's Configuration Management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?
Function 2B: Protect - Identity and Access Management	
26.	To what extent have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been

Function 2B: Protect - Identity and Access Management	
	defined, communicated across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: AC-1, IA-1, and PS-1; NIST SP 800-63-3 and 800-63A, B, and C; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM), OMB M-19-17)?
27.	To what extent does the organization utilize a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities (FICAM, OMB M-19-17; NIST SP 800-53 REV. 4: AC-1 and IA-1; OMB M-19-17, Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; DHS ED 19-01; CSF: PR.AC-4 and 5)?
28.	To what extent has the organization developed and implemented processes for assigning position risk designations and performing appropriate personnel screening prior to granting access to its systems (NIST SP 800-53 REV. 4: PS-2 and PS-3; National Insider Threat Policy; CSF: PR.IP-11, OMB M-19-17)?
29.	To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non-privileged users) that access its systems are completed and maintained (NIST SP 800-53 REV. 4: AC-8, PL-4, and PS-6)?
30.	To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for nonprivileged users to access the organization's facilities [organizationdefined entry/exit points], networks, and systems, including for remote access? (EO 14028, Section 3; HSPD-12; NIST SP 800-53, Rev. 5: AC-17, IA-2, IA-5, IA-8, and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63, 800-157; FY 2022 CIO FISMA Metrics: Section 2; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section A (2); CSF: PR.AC-1 and 6; OMB M19-17, NIST SP 800-157; NIST 800-207 Tenet 6; CIS Top 18 Security Controls v.8: Control 6) **Consistently Implemented (Level 3)** ***Comments***: Consistently Implemented (Level 3) - ED- OIG/I22IT0066 (FISMA Report) The Department's Identity and Access Management Program Needs Improvement
31.	To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access? (EO 14028, Section 3; HSPD-12; NIST SP 800-53, Rev. 5: AC-17 and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63 and 800-157; OMB M-19-17; FY 2022 CIO FISMA Metrics: Section 2; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section A (2); CSF: PR.AC-1 and 6; DHS ED 19-01; NIST 800-207 Tenet 6; CIS Top 18 Security Controls v.8: Control 6) **Managed and Measurable (Level 4)**
32.	To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring

Function 2B: Protect - Identity and Access Management

that privileged user account activities are logged and periodically reviewed? (EO 14028, Section 8; FY 2022 CIO FISMA Metrics: 3.1; OMB M-21-31; OMB M-19-17; NIST SP 800-53, Rev. 5: AC-1, AC2, AC-5, AC-6, AC-17; AU-2, AU-3, AU-6, and IA-4; DHS ED 19-01; CSF: PR.AC-4; CIS Top 18 Security Controls v.8: Controls 5, 6, and 8)

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED- OIG/I22IT0066 (FISMA Report) The Department's Identity and Access Management Program Needs Improvement

33. To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions (NIST SP 800-53 REV. 4: AC-11, AC-12, AC-17, AC-19, AU-2, IA-7, SC-10, SC-13, and SI-4; CSF: PR.AC-3; and FY 2022 CIO FISMA Metrics: 2.10 and 2.11).

34.1. Please provide the assessed maturity level for the agency's Protect - Identity and Access Management program.

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED- OIG/I22IT0066 (FISMA Report) The Department's Identity and Access Management Program Needs Improvement

34.2. Provide any additional information on the effectiveness (positive or negative) of the organization's Identity and Access Management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?

Function 2C: Protect - Data Protection and Privacy

35. To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems (NIST SP 800-122; NIST SP 800-37 (Rev. 2) Section 2.3, Task P-1 ; OMB M-20-04; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J, FY 2020 SAOP FISMA metrics, Sections 1 through 4, 5(b))?

36. To what extent has the organization implemented the 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, as appropriate, throughout the data lifecycle? (EO 14028, Section 3(d); OMB M-22-09, Federal Zero Trust Strategy; NIST 800-207; NIST SP 800-53, Rev. 5; SC-8, SC28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2022 CIO FISMA Metrics: 2.1, 2.2, 2.12, 2.13; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6; CIS Top 18 Security Controls v. 8: Control 3)

Defined (Level 2)

Comments: Defined (Level 2) - ED- OIG/I22IT0066 (FISMA Report) The Department's Data Protection and Privacy Program Needs Improvement

Function 2C: Protect - Data Protection and Privacy

37. To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (FY 2022 CIO FISMA Metrics, 5.1; NIST SP 800-53, Rev. 5: SI3, SI-7, SI-4, SC-7, and SC-18; DHS BOD 18-01; DHS ED 19- 01; CSF: PR.DS-5, OMB M-21-07; CIS Top 18 Security Controls v.8: Controls 9 and 10)

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED- OIG/I22IT0066 (FISMA Report) The Department's Data Protection and Privacy Program Needs Improvement

38. To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events? (NIST SP 800-122; NIST SP 800-53 REV. 4: Appendix J, SE-2; FY 2020 SAOP FISMA metrics, Section 12; OMB M-17-12; and OMB M-17-25)?

39. To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training (NIST SP 800-53 REV. 4: AR-5, FY 2020 SAOP FISMA Metrics, Sections 9 10, and 11)

40.1. Please provide the assessed maturity level for the agency's Protect - Data Protection and Privacy program.

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED- OIG/I22IT0066 (FISMA Report) The Department's Data Protection and Privacy Program Needs Improvement

40.2. Provide any additional information on the effectiveness (positive or negative) of the organization's 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?

Function 2D: Protect - Security Training

41. To what extent have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated across the agency, and appropriately resourced? (Note: this includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant security responsibilities (NIST SP 800-53 REV. 4: AT-1; and NIST SP 800-50).

42. To what extent does the organization utilize 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? (FY 2022 CIO FISMA Metrics, Section 6; NIST SP 800-53, Rev. 5: AT-2, AT-3, and PM-13; NIST SP 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; and CIS Top 18 Security Controls v.8: Control 14)

Function 2D: Protect - Security Training	
	Managed and Measurable (Level 4)
43.	To what extent does the organization utilize a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to its culture? (Note: the strategy/plan should include the following components: the structure of the awareness and training program, priorities, funding, the goals of the program, target audiences, types of courses/material for each audience, use of technologies (such as email advisories, intranet updates/wiki pages/social media, web based training, phishing simulation tools), frequency of training, and deployment methods (NIST SP 800-53 REV. 4: AT-1; NIST SP 800-50: Section 3; CSF: PR.AT-1).
44.	To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST SP 800-53 REV. 4: AT-2; FY 2022 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-2; SANS Top 20: 17.4).
45.	To what extent does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures) (NIST SP 800-53 REV. 4: AT-3 and AT-4; FY 2022 CIO FISMA Metrics: 2.15)?
46.1.	Please provide the assessed maturity level for the agency's Protect - Security Training program. Managed and Measurable (Level 4)
46.2.	Please provide the assessed maturity level for the agency's Protect function. Managed and Measurable (Level 4)
46.3.	Provide any additional information on the effectiveness (positive or negative) of the organization's 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?
Function 3: Detect - ISCM	
47.	To what extent does the organization utilize information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier? (NIST SP 800-53, Rev. 5: CA-7, PM-6, PM-14, and PM-31; NIST SP 800-37 (Rev. 2) Task P-7; NIST SP 800-137: Sections 3.1 and 3.6; CIS Top 18 Security Controls v.8: Control 13) Managed and Measurable (Level 4)
48.	To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: CA-1; NIST SP 800-137; CSF: DE.DP-1; NIST 800-37, Rev. 2

Function 3: Detect - ISCM	
	Task P-7 and S-5)
49.	How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls? (OMB A-130; NIST SP 800-137: Section 2.2; NIST SP 800-53, Rev. 5: CA-2, CA-5, CA-6, CA-7, PL-2, and PM-10; NIST Supplemental Guidance on Ongoing Authorization; NIST SP 800-37 (Rev. 2) Task S-5; NIST SP 800-18, Rev. 1, NIST IR 8011; OMB M-14-03; OMB M-19-03) **Managed and Measurable (Level 4)**
50.	How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?
51.1.	Please provide the assessed maturity level for the agency's Detect - ISCM domain/function. **Managed and Measurable (Level 4)**
51.2.	Provide any additional information on the effectiveness (positive or negative) of the organization's ISCM program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?
Function 4: Respond - Incident Response	
52.	To what extent does the organization utilize an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents (NIST SP 800-53 REV. 4: IR-8; NIST SP 800-61 Rev. 2, section 2.3.2; CSF, RS.RP-1, Presidential Policy Directive (PPD) 8 - National Preparedness)?
53.	To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; CSF, RS.CO-1, OMB M-20-04; FY 2022 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?
54.	How mature are the organization's processes for incident detection and analysis? (EO 14028, Section 6; OMB M-22-05, Section I; CISA Cybersecurity Incident and Vulnerability Response Playbooks; FY 2022 CIO FISMA Metrics: 10.6; NIST 800-53, Rev. 5: IR-4, IR-5, and IR-6; NIST SP 800-61 Rev. 2; OMB M20-04; CSF: DE.AE-1, DE.AE-2 -5, PR.DS-6, RS.AN-1 and 4, and PR.DS-8; and CIS Top 18 Security Controls v.8: Control 17) **Consistently Implemented (Level 3)** ***Comments***: Consistently Implemented (Level 3) - ED- OIG/I22IT0066 (FISMA Report) The Department's Incident Response Program Needs Improvement

Function 4: Respond - Incident Response

55. How mature are the organization's processes for incident handling? (EO 14028, Section 6; OMB M-22-05, Section I; CISA Cybersecurity Incident and Vulnerability Response Playbooks; FY 2022 CIO FISMA Metrics: 10.6; NIST 800-53, Rev. 5: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2)

Managed and Measurable (Level 4)

56. To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-20-04; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 5; DHS Cyber Incident Reporting Unified Message)

57. To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support (NIST SP 800-86; NIST SP 800-53 REV. 4: IR-4; OMB M-20-04; PPD-41).

58. To what extent does the organization utilize the following technology to support its incident response program? Web application protections, such as web application firewalls Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools Aggregation and analysis, such as security information and event management (SIEM) products Malware detection, such as antivirus and antispam software technologies Information management, such as data loss prevention File integrity and endpoint and server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2; NIST SP 800-44)

59.1. Please provide the assessed maturity level for the agency's Respond - Incident Response domain/function.

Managed and Measurable (Level 4)

59.2. Provide any additional information on the effectiveness (positive or negative) of the organization's Incident Response program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the incident response program effective?

Function 5: Recover - Contingency Planning

60. To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined and communicated across the organization, including appropriate delegations of authority (NIST SP 800-53 REV. 4: CP-1, CP-2, and CP-3; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?

61. To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts? (FY 2022 CIO FISMA Metrics: 10.1.4; NIST SP 800-53, Rev. 5: CP-2, and RA-9; NIST SP 800-34, Rev. 1, 3.2; NIST IR 8286; FIPS 199; FCD-1; OMB M-19-03; CSF:ID.RA-4)

Managed and Measurable (Level 4)

62. To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated

Function 5: Recover - Contingency Planning	
	with other continuity plans (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34; FY 2022 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?
63.	To what extent does the organization perform tests/exercises of its information system contingency planning processes? (FY 2022 CIO FISMA Metrics: 10.1; NIST SP 800-34; NIST SP 800-53, Rev. 5: CP-3 and CP-4; CSF: ID.SC-5 and CSF: PR.IP10; CIS Top 18 Security Controls v.8: Control 11) **Managed and Measurable (Level 4)**
64.	To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST SP 800-53 REV. 4: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD-1; NIST CSF: PR.IP-4; FY 2022 CIO FISMA Metrics, Section 5; and NARA guidance on information systems security records)?
65.	To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk based decisions (CSF: RC.CO-3; NIST SP 800-53 REV. 4: CP-2 and IR-4)?
66.1.	Please provide the assessed maturity level for the agency's Recover - Contingency Planning domain/function. **Managed and Measurable (Level 4)**
66.2.	Provide any additional information on the effectiveness (positive or negative) of the organization's 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?

APPENDIX A: Maturity Model Scoring

A.1. Please provide the assessed maturity level for the agency's Overall status.

Summary

Cycle	Maturity Level	Mean	Mode
FY22 Core Metrics	Managed and Measurable (Level 4)	3.61	Managed and Measurable (Level 4)
FY22 Supplementary Metrics			
FY22 Overall	Managed and Measurable (Level 4)	3.61	Managed and Measurable (Level 4)

Overall

Function	Calculated Maturity Level	Mean	Mode	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management / Supply Chain Risk Management	Consistently Implemented (Level 3)	3.33	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3) - ED- OIG/I22IT0066 (FISMA Report) The Department's Risk Management and Supply Chain Risk Management Program Needs Improvement
Function 2: Protect - Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training	Managed and Measurable (Level 4)	3.46	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	
Function 3: Detect - ISCM	Managed and Measurable (Level 4)	4.00	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	
Function 4: Respond - Incident Response	Managed and Measurable (Level 4)	3.89	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	

APPENDIX A: Maturity Model Scoring				
Function 5: Recover - Contingency Planning	Managed and Measurable (Level 4)	4.44	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)
Function 0: Overall	Effective	3.61	Managed and Measurable (Level 4)	Effective

Appendix E. Acronyms and Abbreviations

Department	U.S. Department of Education
FISMA	Federal Information Security Modernization Act of 2014
FSA	Federal Student Aid
FY	fiscal year
ICAM	Identity, Credential, and Access Management
ISCM	Information Security Continuous Monitoring
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIVOT	Portfolio of Integrated Value-Oriented Technologies
SP	Special Publication

Appendix F. Department Comments

UNITED STATES DEPARTMENT OF EDUCATION

DATE: July 26th, 2022

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

FROM: Jason Gray
Chief Information Officer
Department of Education

SUBJECT: Response to Draft Audit Report
The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2022
Control Number ED-OIG/I22IT0066

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) Report, Audit of the U.S. Department of Education's Federal Information Security Modernization Act (FISMA) of 2014 Report for Fiscal Year (FY) 2022 Draft Report, Control Number ED-OIG/I22IT0066. The Department recognizes the objective of the annual OIG FISMA audit is to evaluate and determine the effectiveness of the Department's information security program policies, procedures, and practices. We appreciate OIG's exceptional efforts to provide strategic and meaningful recommendations while balancing substantial changes in methodology and timelines this year. We also appreciate the recognition of the Departments commitment, and our ongoing progress, to strengthen the overall cybersecurity of its networks, systems, and data, as reflected in the draft report.

During the first half of FY 2022, the Office of the Chief Information Officer (OCIO) successfully continued to support IT services to support nearly 100% telework in response to the COVID-19 pandemic. However, during the second half of FY 2022, The Department shifted from nearly 100% telework to a hybrid telework posture. Throughout this transition, there was no significant impact or compromise to the Department Information Security Program, and the Department continued execution of missions without interruption. Additionally, despite the challenging work environment necessitated by the COVD-19 pandemic and the evolving technology changes to meet working requirements, the Department did not have any major information security incidents occur. To continue strengthening our cloud portfolio, the Department has continued its close working relationship with the FedRAMP Project Management Office (PMO) which established increased reoccurring continuous monitoring meetings with participating agencies to help improve the security posture of those Cloud Service Providers.

In February 2022, the Department implemented a new cybersecurity policy framework aligned with Executive Order (EO) 14028 Improving the Nation's Cybersecurity and National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5. The updated framework ensures a more comprehensive inventory of policies that directly align with the latest catalog of security control families and requirements levied through EO 14028. Five Instructions and 22 Standards have been converted into 20 new Standards (control families) aligned with the Cybersecurity Framework (CSF) and NIST 800-53, Revision 5. The framework modernizes the Department's cybersecurity policies, enables system stakeholders to easily find Department of Education (ED) requirements, allows for updates to the Department's system of record for FISMA reporting, Cyber Security Assessment and Management

System (CSAM) with ED defined control parameters to support System Security Plan (SSP) development and assessments, includes control overlays for requirements not within 800-53 control baselines, and enhances maintenance and strengthens ability to rapidly update for new requirements while maintaining mapping to CSF and NIST controls.

The Department released a memorandum on Plan of Action & Milestones (POA&M) criticality on September 30, 2021, in response to the IG recommendation from FY 2020, closing Corrective Action Plan (CAP) 1.1. The Department has engaged significant development of user-defined criticality for all new and existing information systems, entered into CSAM to consistently capture and report on in alignment with the NIST SP800-53 control mapping.

The Department's Security Assessment Team (SAT) worked with the Office of the Chief Information Security Officer (OCIO) to implement the Ongoing Security Assessment & Authorization (OSA) program, which started in December 2021. The OSA program and method of assessment replaced the older static-point-in-time assessment model of Assessment & Authorization (A&A). The threshold for entry into the OSA program is a risk assessment that focuses on the following areas: system demonstration, control baseline and inheritance review, and the Department's CSF Scorecard and discrepancy reports. The OSA program will reduce steps and modify artifacts to improve efficiency. The overall outcome is more frequent system stakeholder engagement and timely risk visibility.

The Department released Standard PR.DS: Protection of Federal Tax Information. Released in January 2022, this standard establishes the ED standards for safeguarding the confidentiality of Federal Tax Information (FTI) as required by Internal Revenue Service (IRS) Safeguards Program1 and IRS Publication 1075, Tax Information Security and Privacy Guidelines for Federal, State and Local Agencies. In accordance with Internal Revenue Code (IRC), Section 6103(p)(4)3; and IRS Publication 1075, as a condition of receiving FTI directly from either the IRS or from secondary sources.

Throughout the year, we continued our outreach and risk communications by disseminating monthly "State of IT" reports to the Department's senior leaders. These executive-level reports provide the Department's senior leaders with a holistic view of their IT investments, services, and cybersecurity posture through comprehensive IT and cybersecurity trends, metrics, and key insights to prompt top-down engagement and actions. These reports prepare senior Principal Operating Component (POC) leaders for the Monthly Deputy Secretary cybersecurity briefings facilitated by the Department CISO. The meeting communicates Department cyber risks, trends, metrics, key insights, upcoming announcements, and actions.

The Department continued to mature its risk management processes through enhancements to the CSF Risk Scorecard. POC leadership can now monitor status of program-level business continuity planning and testing activities. These enhancements allowed ED to close CAP 8.3 from the FY 2020 FISMA audit and are targeted to result in consistent implementation of business continuity planning activities. In FY 2022 Quarter 1, the Department enhanced its Power BI reporting to track and report compliance to ED 14028 mandates including, but not limited to, Multifactor Authentication (MFA), encryption, resiliency, etc. The FISMA Dashboard was also enhanced to visualize compliance statuses against recently released FY 2022 CIO Metrics reporting guidelines (v1.1), issued by OMB/CISA in support of EO 14028 requirements.

In FY 2022, the Department was approached to provide a demonstration of its cybersecurity risk scoring and visualization capabilities to several partner Federal Departments. As a result of the Department's demonstration of risk scoring and visualization capabilities, the Partner Departments have expressed began establishing similar capabilities within their cybersecurity mission space.

The Department established a Vulnerability Disclosure Policy (VDP) program in FY 2021, to provide an open channel and legal safe harbor for the discoverer of vulnerabilities to report it to the Department. The VDP allows the research community and others to alert the Department about vulnerabilities in its systems through a clearly established program. The Department expanded the VDP program in FY 2022 Q1 to cover all internet accessible Department systems. Information submitted to the Department under the VDP will be used to mitigate or remediate internet-accessible systems and services vulnerabilities, or vendor's internet-accessible systems or services.

In response to the January 2022 Apache Log4j vulnerability, the Department Vulnerability Management (VM) team identified all impacted systems, assets, and remediation actions. All reports were forwarded to the EDSOC for further incident response activities. The EDSOC coordinated across the Department (FSA SOC, CSOC, etc.) to identify impacted assets, patch immediately, block indicators of compromise, and take necessary incident response actions if compromises were discovered. The EDSOC completed all network traffic and forensics analysis on ED systems and concluded that no Department assets showed indication of a successful compromise. The Department was selected to participate in the first Cybersecurity Safety Review Board analysis of log4j and was cited as providing the most input and support of Federal Cabinet-level Departments.

In response to Emergency Directive 22-03 Mitigate VMWare Vulnerabilities, the Department issued a Chief Information Security Officer (CISO) Memorandum on May 20, 2022. Information System Owners (ISOs) and Information System Security Officers (ISSOs) were required to enumerate all instances of impacted VMware products within their system authorization boundaries, report findings to the OCIO Vulnerability Management team, and deploy updates (or remove the VMWare product until an update is available). There were no findings of impact to the Department, which was reported to CISA.

On May 5, 2020, to address the closure and limited operating capacity of Federal Government badging offices due to the Coronavirus (COVID-19), the Department issued Standard PR.AC: Emergency PIV Alternative Standard. This memorandum served to drive actions necessary to ensure the Department's workforce is using the strongest multifactor authentication possible in alignment with Executive Order 14028. The Department released a follow up CISO Memorandum on April 15, 2022, rescinding Standard PR.AC: Emergency PIV Alternative Standard as required by Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors (HSPD-12), all federal employees and contractors are required to use a Personal Identification Verification (PIV) smartcard (badge) for authentication and access to Federal facilities and IT systems.

The Department took immediate action in Q1 and Q2 regarding M-22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles by creating, funding, and onboarding a GS-15 zero-trust architecture (ZTA) program manager and releasing a Department Strategy and project schedule for full implementation by the end of FY 2024. The Department received the initial transfer of $15M in TMF funds, used to establish a ZTA PMO, engage the recompete of Enterprise Identity, Credential, and Access Management (ICAM), and obtain Secure Access Service Edge (SASE) & Security Orchestration Automation & Response (SOAR) capabilities. There is ongoing collaboration between ZTA, ICAM, Enterprise Detection and Response (EDR), and Cyber Data Lake (CDL) PMOs to fulfill progress towards all pillars of Zero Trust. A "zero trust" approach to security provides the Department with a necessary and defensible architecture against increasingly sophisticated cyber-attacks. The Department is on track to meet the requirements set forth by OMB and maintain a resilient cybersecurity posture.

OCIO completed a 90-day sprint, tasked by the Office of Management and Budget (OMB) in response to EO 14028, on Multifactor Authentication (MFA) Encryption for the Data at Rest (DAR) and Encryption for the Data in Transit (DIT). The Department targets to complete the OMB requirements by December 31, 2022.

The Department updated our internal vulnerability management procedures in accordance with BOD 22-01 Reducing the Significant Risk of Known Exploited Vulnerabilities. The Department continues to remediate each vulnerability according to the timelines set forth in the CISA-managed vulnerability catalog. The Department is working with CISA to mature our Continuous Diagnostics and Mitigation (CDM) capabilities to augment and enhance remediation actions as required by this directive.

In support of Security Operations Center (SOC) consolidation and maturation, the Department continues to identify task separation, integrate security tooling, coordinate incident investigation and response, and remove duplication between the Department's two SOCs, EDSOC and FSA SOC. Existing milestones include refining current processes that support incident response and management to be aligned to a singular source, establishing automation within our incident response tool, and evolving training on newly enhanced processes and technologies. In FY 2021, the SOC maturation plan was updated to address key requirements levied on the Department in support of the recently released Executive Order (EO) 14028 on Improving the Nation's Cybersecurity and NIST 800-53 Rev. 5. Updates to the plan in FY 2022 will result in improved incident response (IR) maturation in keeping within Federal IR requirements, continued improvement to our data loss prevention systems, increased cost savings through virtualization, and increased use of specialized personnel dedicated to threat intelligence analysis, Law Enforcement cooperation, and Hunt Team activities, providing a more robust a complete threat analysis product to our customer.

Below are responses that address each recommendation in the Draft Report. The Department will address each finding and recommendation in the corrective action plans provided and as agreed upon by your office.

REPORTING METRIC DOMAIN No.3: CONFIGURATION MANAGEMENT

The OIG recommends that the Chief Information Officer require the Department to:

OIG Recommendation 1.1: Implement additional measures for patches to be prioritized and applied within required timeframes.

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2023 and will develop a corrective action plan by September 30, 2022 to address the recommendation.

OIG Recommendation 1.2: Establish additional oversight controls to update, remove, or replace obsolete or unsupported solutions and encryption protocols.

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2023 and will develop a corrective action plan by September 30, 2022 to address the recommendation.

REPORTING METRIC DOMAIN No.4: IDENTITY AND ACCESS MANAGEMENT

The OIG recommends that the Chief Information Officer require the Department to:

OIG Recommendation 2.1: The Contracting Officer Representative sign, complete, and maintain Position Risk Designation forms for background investigations.

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2023 and will develop a corrective action plan by September 30, 2022 to address the recommendation.

OIG Recommendation 2.2: Review Active Directory user accounts to enforce policy compliance for password expiration and account deactivation.

Management Response: The Department partially concurs with this recommendation. Active Directory (AD) Password enforcement settings and scripts are in use for account disablement per SOP. The Department will do deep-dive to ensure policy compliance and develop a corrective action plan by September 30, 2022 to address any gaps.

OIG Recommendation 2.3: Remove terminated users' access to Department resources in accordance with Departmental policy.

Management Response: The Department partially concurs with this recommendation. Four accounts were terminated properly by offboarding workflow process last year. Those four accounts were temporarily enabled for an Enterprise Vault (EV) email migration this spring. The Department will develop a corrective action plan by September 30, 2022, to improve and explain the process.

OIG Recommendation 2.4: Establish and enforce a policy to maintain and track all privileged accounts in authorized Privileged Access Management System(s).

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2023 and will develop a corrective action plan by September 30, 2022 to address the recommendation.

OIG Recommendation 2.5: Establish and enforce a corrective action plan to monitor and remediate identified database vulnerabilities.

Management Response: The Department partially concurs with this recommendation. The Department immediately resolved three of the findings identified. Of the remaining findings the Department believes they will be resolved through evaluating the vendor configuration against the Department's STIG Policy. FSA will develop a corrective action plan by September 30, 2022 to address the recommendation.

REPORTING METRIC DOMAIN No.5: DATA PROTECTION AND PRIVACY

The OIG recommends that the Chief Information Officer require the Senior Agency Official for Privacy to:

OIG Recommendation 3.1: Implement monitoring and oversight controls to ensure media sanitization policies and processes are in place and document evidence of the disposal or reuse of all used digital media.

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2023 and will develop a corrective action plan by September 30, 2022, to address the recommendation.

OIG Recommendation 3.2: Update digital media sanitization policies and processes to include all requirements outlined in Federal regulations.

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2023 and will develop a corrective action plan by September 30, 2022, to address the recommendation.

REPORTING METRIC DOMAIN No.8: INCIDENT RESPONSE

The OIG recommends that the Chief Information Officer require the Department to:

Recommendation 4.1: Establish oversight controls to ensure that the Department follows United States Computer Emergency Readiness Team required notification guidelines, timeframes, as well as communicating the relevant incidents to the OIG.

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2023 and will develop a corrective action plan by September 30, 2022, to address the recommendation.

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

cc:

Gary Stevens, Deputy Chief Information Officer, Office of the Chief Information Officer
Steven Hernandez, Director, Information Assurance Services, Office of the Chief Information Officer
Margaret Glick, FSA Chief Information Officer, Federal Student Aid
Dan Commons, Director, FSA Deputy Chief Information Officer, Federal Student Aid
Devin Bhatt, Acting FSA Chief Information Security Officer, Federal Student Aid
Sam Rodeheaver, Audit Liaison, Office of the Chief Information Officer
Stefanie Clay, Audit Liaison, Federal Student Aid
Bucky Methfessel, Senior Counsel for Information & Technology, Office of the General Counsel
Kala Surprenant, Senior Counsel for Oversight, Office of the General Counsel
April Bolton-Smith, Post Audit Group, Office of the Chief Financial Officer
L'Wanda Rosemond, AARTS Administrator, Office of Inspector General