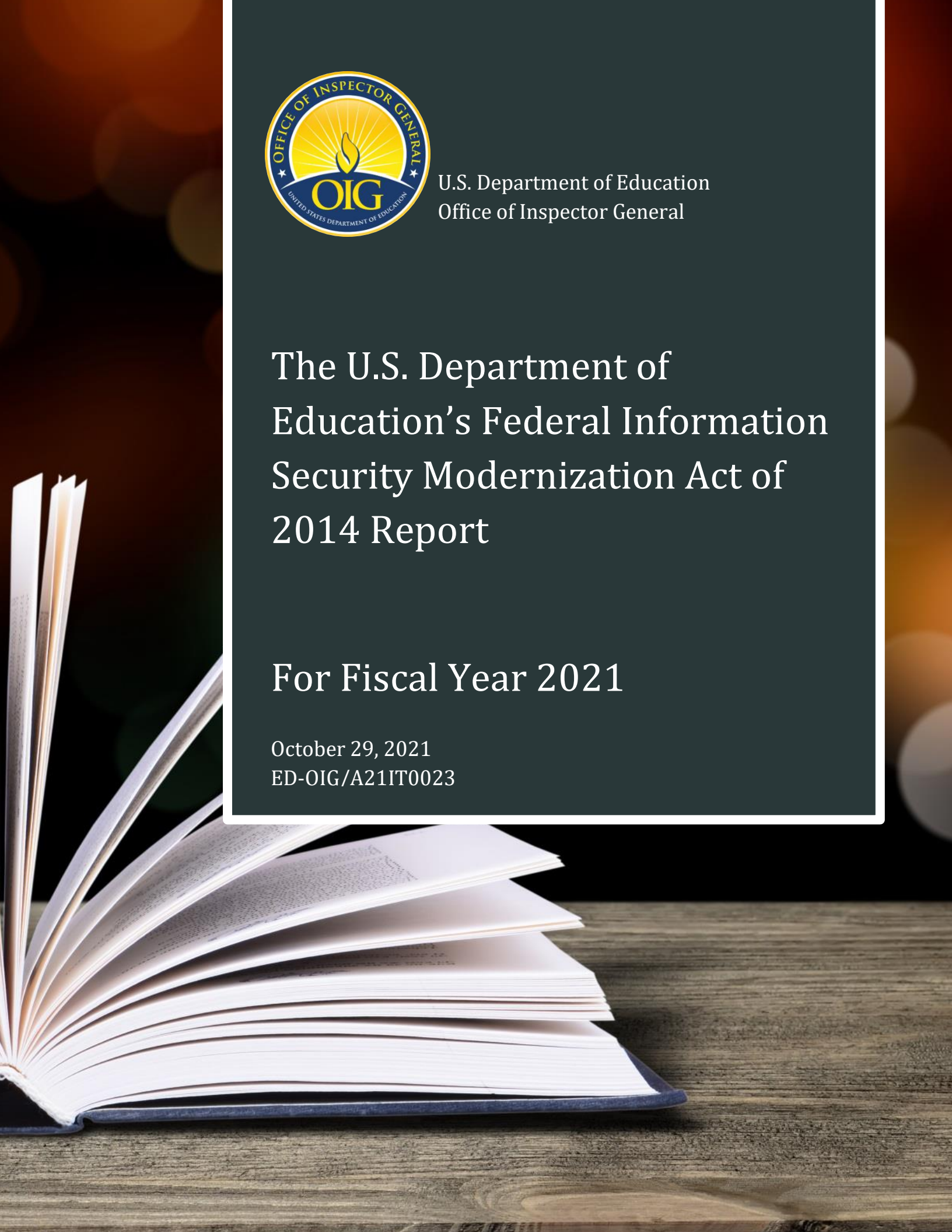


U.S. Department of Education
Office of Inspector General

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

For Fiscal Year 2021

October 29, 2021
ED-OIG/A21IT0023

NOTICE

Statements that managerial practices need improvements, 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.

October 29, 2021

TO: Jason K. Gray
Chief Information Officer

FROM: Robert D. Mancuso /s/
Assistant Inspector General
Information Technology, Audits and Computer Crime Investigations
Office of Inspector General

SUBJECT: Final Audit Report
The U.S. Department of Education's Federal Information Security Modernization Act of 2014 for Fiscal Year 2021
Control Number ED-OIG/A21IT0023

Attached is the subject final audit 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 2021. 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 audit 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 at 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
Steven Hernandez, Chief Information Security Officer, Office of the Chief Information Officer

Daniel Commons, Director, Enterprise Cybersecurity Group, Chief Information Security Officer, Federal Student Aid
Samuel Rodeheaver, Audit Liaison, Office of the Chief Information Officer
Stefanie Clay, Audit Liaison, Federal Student Aid
Michael Gardner, Deputy Chief Information Security Officer, Federal Student Aid
Devin Bhatt, Deputy Chief Information Security Officer, 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 determine whether the U.S. Department of Education's (Department) overall information technology (IT) security programs and practices were effective as they relate to Federal information security requirements. In fiscal year (FY) 2020, we focused our audit efforts solely on Departmental Systems. This year, we focused on five Federal Student Aid (FSA) Systems and the Department's implementation of recommendations from previous reports.

To answer this objective, we rated the Department's performance in accordance with FY 2021 Inspector General (IG) Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics. 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 National Institute of Standards and Technology's (NIST) "Framework for Improving Critical Infrastructure Cybersecurity." Following the SolarWinds Supply Chain Attack in December 2020, the FY 2021 IG FISMA Reporting Metrics introduced Supply Chain Risk Management as a separate metric to prompt the agency preparations for these types of attacks.

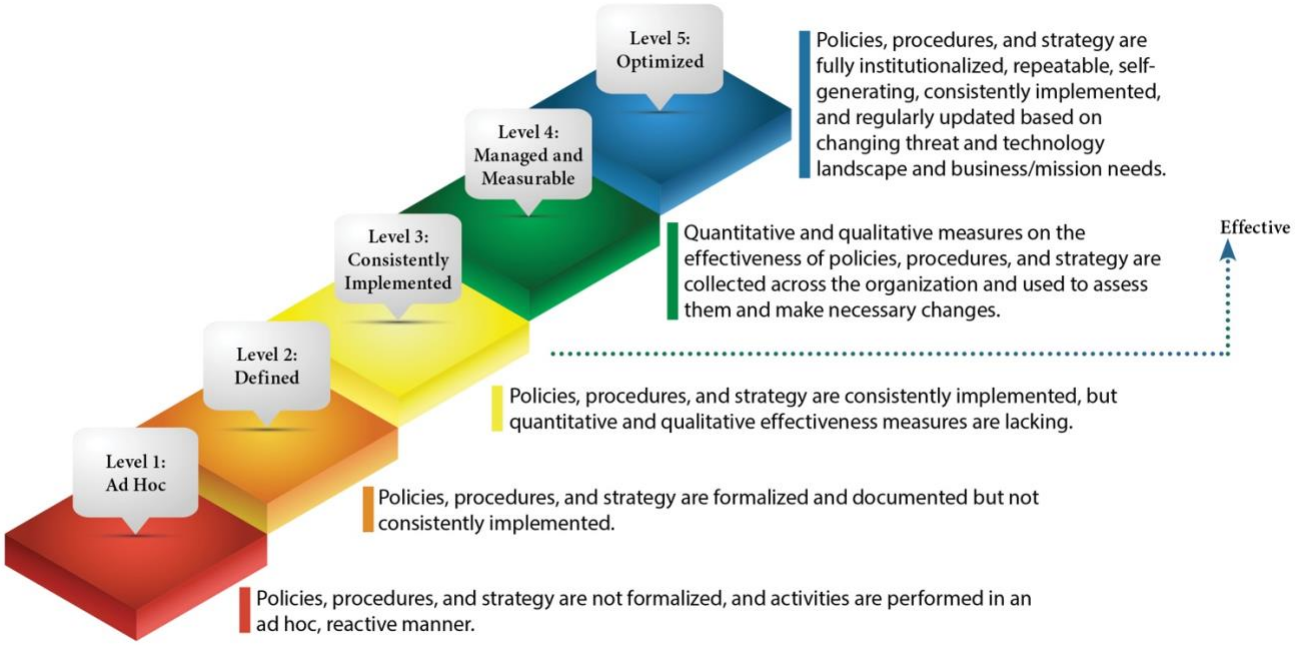
Table 1. Cybersecurity Framework Functions, Definitions and Domains

Framework Function	Definition	Domains
Identify	Develops the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities	Risk Management **Supply Chain Risk Management**
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
Detect	Develops and implements the appropriate activities to identify the occurrence of a cybersecurity event	Information Security Continuous Monitoring
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
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

Since the FY 2017 FISMA reporting process, IGs have been directed to utilize 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. To further help evaluate the impact of these metrics and prepare agencies for the possibility of changing the calculation process in the future, the FY 2021 IG FISMA Reporting Metrics introduced a pilot concept of weighting specific FISMA metrics for assessment and scoring. As part of the proposed weighted average approach to scoring, certain metrics would be weighted twice as much in the maturity calculation.

In accordance with the FY 2021 IG FISMA Metrics, IGs assess the effectiveness of each security function using a maturity model approach, developed as a collaborative effort amongst the Council of the Inspectors General on Integrity and Efficiency, the Office of Management and Budget, and the Department of Homeland Security. Figure 1 identifies the five maturity levels (with each succeeding level representing a more advanced level of implementation).

Figure 1. The Five Maturity Levels



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 level.

What We Found

The Department made several improvements in implementing its cybersecurity posture. In FY21 the Department improved in three functional areas and three metric areas from Level 2 Defined to Level 3 Consistently Implemented.

Table 2. Improvements by Security Function

Security Function	FY2020 Maturity Level	FY2021 Maturity Level
Identify	Defined	**Consistently Implemented**
Protect	Defined	**Consistently Implemented**
Detect	Defined	**Consistently Implemented**
Respond	Consistently Implemented	Consistently Implemented
Recover	Consistently Implemented	Consistently Implemented

However, its overall IT security programs and practices were not effective in all the five security functions. We had findings in four of the nine metric domains, which included findings with the same or similar conditions identified in prior reports, as well as open findings from previous years where the corrective action plan was not completed.

We determined the Department's programs were consistent with

- **Level 2—Defined,** which is considered not effective for three domains: Supply Chain Risk Management, Identity and Access Management, and Data Privacy and Protection.
- **Level 3—Consistently Implemented,** which is considered not effective for six domains: Risk Management, Configuration Management, Security Training, Information System Continuous Monitoring, Incident Response, and Contingency Planning.

None of the Department domains were rated **Level 1, Ad-Hoc**, which has the greatest risks. Also, the Risk Management, Security Training and Information Security Continuous Monitoring metric areas improved from **Level 2, Defined** (cited during our FY 2020 audit), to **Level 3, Consistently Implemented**.

For FY 2021, the Department has improved on several individual metric scoring questions, especially in the areas of Risk Management, Configuration Management, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning. The Department also demonstrated improvement in its processes from FY 2020 within several metric areas. Appendix B shows the six metric domains improvements along with all the Department's metric maturity level ratings by domain and by the number of questions for FYs 2020 and 2021.[1]

Although the Department made considerable progress in strengthening its information security programs, we found areas needing improvement in all nine metric domains. Specifically, we found that the Department can strengthen its controls in the following areas:

- **Risk Management**. Remediation process for its Plan of Action and Milestones; information security architecture integration with the supply chain strategy, IT inventory reporting; and required IT security clauses for its contracts (see Finding 1).
- **Supply Chain Risk Management [New].** Develop and implement an enterprise supply chain assessment strategy (see Finding 2).
- **Configuration Management.** Use of unsecure connections and appropriate application connections protocols; reliance on unsupported operating systems (see Finding 3).
- **Identify and Access Management**. Implementing the Identity, Credential, and Access Management tool; properly document its risk position designation records; lack of enforcement for 30-minute time-out, recertification of user access, missing website warning banners, and lack of two factor authentication enforcement (see Finding 4).
- **Data Protection and Privacy.** Ensuring consistent documentation of Privacy Impact Assessments and System of Records Notices and implementing digital media sanitization policies (see Finding 5).

[1] The FY 2021 IG FISMA Reporting Metrics removed or combined several questions for Risk Management, Identity and Access Management, Security Training, Information Security Continuous Monitoring, and Contingency Planning domains. As a result, the number of questions in these sections are slightly different than those required in the FY 2020 FISMA.

- **Security Training**. Establishing monitoring and oversight controls that ensure all new users satisfy all the mandatory training requirements before they receive access to Departmental resources (see Finding 6).

- **Information Security Continuous Monitoring**. Establishing oversight controls to review, monitor, and verify progress of the ISCM strategy. Conduct annual reviews of all Departmental cyber security policies, to align it with the current environment (see Finding 7).

- **Incident Response.** Ensuring the Department's data loss prevention solution is properly configured, and functions as intended (see Finding 8).

- **Contingency Planning**. Improving oversight controls to ensures contingency plan tests, and other artifacts impacting contingency plan testing, are documented, and updated in a consistent and timely manner. Developing controls to confirm the proper validation and verification of all required contingency planning controls (see Finding 9).

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.

We followed up on the status of prior year findings and the implementation of corrective actions from the last three FISMA audits (FY 2018–FY 2020) to verify that the Department had addressed past deficiencies. See Appendix C, Status of Prior-Year Recommendations, for additional details.

Our answers to the questions in the FY 2021 IG FISMA Metrics template that will be used for the CyberScope report, are shown in Appendix D. All Federal agencies are to submit their IG FISMA metric determinations into the Department of Homeland Security's CyberScope application by October 29, 2021.

What We Recommend

We made 16 recommendations in 4 of the 9 metric domains to assist the Department with increasing the effectiveness of their information security programs. We are not making new recommendations for five metric domains due to open recommendations from prior years. The implementation of corrective action plans will help the Department fully comply with all applicable requirements of FISMA, the Office of Management and Budget, the Department of Homeland Security, and the National

Institute of Standards and Technology. 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	Domain	Recommendations
Identify	Risk Management Supply Chain Risk Management	NA
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training	15
Detect	Information Security Continuous Monitoring	NA
Respond	Incident Response	1
Recover	Contingency Planning	NA

Department Comments and Our Response

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

Introduction

Purpose

We performed this audit based on requirements specified within the Federal Information Security Modernization Act of 2014 (FISMA) and the Fiscal Year (FY) 2021 Inspector General (IG) FISMA Metrics V 1.1 (FY 2021 IG FISMA Metrics), issued on May 12, 2021. Our audit focused on reviewing the five security functions and nine associated metric domains for cybersecurity management.

Background

FISMA, part of the E-Government Act of 2002 (Public Law 107-347),[2] 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, commonly referred to as FISMA,[3] 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 IGs. 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

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

[3] 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.

modifications that modernize Federal security practices to address evolving security concerns. These changes result in less overall reporting, stronger use of continuous monitoring in systems, increased focus on the agencies for compliance, and reporting that is more focused on the issues caused by security incidents. Furthermore, OMB regulations require Federal agencies to ensure that appropriate officials are assigned security responsibilities and periodically review their information systems' security controls.

The FY 2021 IG FISMA Metrics in alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework establishes 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. 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. Specifically, the agency's chief information officer is required to oversee the program.

FISMA requires agencies to have an independent evaluation of their information security programs and practices conducted annually and to report the results to OMB. FISMA states that the independent evaluation is to be performed by the agency IG or an independent external auditor. FISMA requires the Office of Inspector General (OIG) to assess the effectiveness of the agency's information security program. FISMA specifically mandates that each independent evaluation must include testing 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 2021 Inspector General FISMA Reporting Metrics

The Council of the Inspectors General on Integrity and Efficiency, OMB, and Department of Homeland Security developed the FY 2021 IG FISMA Metrics in consultation with the Federal Chief Information Officer Council. The FY 2021 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." Using the FY 2021 IG FISMA Metrics, IGs 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, IGs determine the overall agency rating and the rating for each of the Cybersecurity Framework Functions at the maturity level.

The FY 2021 IG FISMA Metrics introduced a pilot concept of weighting specific FISMA metrics for assessment and scoring based on the priority metrics and a combination of the lowest average performing metrics from previous assessments, administration priorities, and the highest value controls. As part of the proposed weighted average approach to scoring, these priority metrics would be weighted twice as much in the maturity calculation. The overall maturity of the agency's information security program would be calculated based on the average rating of the individual function areas. The outcomes of this pilot will be shared with the Chief Information Security Officer council and the Council of the Inspectors General on Integrity and Efficiency for further consideration.

In accordance with FISMA and OMB Memorandum M-21-02, *Fiscal Year 2020–2021 Guidance on Federal Information Security and Privacy Management Requirements*, all Federal agencies are to submit their IG metrics into the Department of Homeland Security's CyberScope application by October 29, 2021, included in Appendix D.

Department's Information Technology Investments

The U.S. Department of Education's (Department) FY 2021 total spending for information technology (IT) investments was estimated at $1 billion, which included $608 million in spending on major IT investments (68 percent of total spending). This is an 18.4 percent increase from the FY 2020 total spending of $844 million. 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

In early 2019, the Department began procuring most of its IT infrastructure services and items through a portfolio of multiple contracts within performance-based contracts called Portfolio of 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,[4] 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

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

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 2020 FISMA audit, we identified 24 recommendations (8 of which were repeat recommendations) in all 8 metric domains that addressed the conditions noted in the report, with most of the recommendations made in the Identify and Protect security functions. The Department concurred with 5 recommendations, partially concurred with 16 recommendations, and did not concur with 3 recommendations. As of July 2021, the Department and FSA reported that they had completed corrective actions for 4 of the 24 recommendations. The Department and FSA are currently scheduled to complete all the remaining corrective actions by the end of FY 2021, with some recommendations extended to the end of 2022.

See Appendix C for complete details regarding prior year FISMA audit recommendations, and the status of corrective actions for FYs 2018, 2019, and 2020.

Audit Results and Findings

We had findings in four of the nine metric domains within the five security functions—Identify, Protect, Detect, Respond, and Recover. Our findings in the metric domains included findings with the same or similar conditions identified in OIG reports issued from FYs 2018 through 2020, and therefore we decided to reopen these recommendations so the Department can take further action to correct the problems identified.

SECURITY FUNCTION 1—IDENTIFY

The Identify security function is comprised of the Risk Management and Supply Chain Risk Management (SCRM) metric domains[5]. 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 program, we noted that improvements were needed in the Department's corrective action plan remediation process, supply chain strategy, information security architecture integration with the supply chain strategy, IT inventory reporting, and the inclusion of IT security clauses for its contracts.

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 determined that the Department's risk management program was consistent with the Consistently Implemented level (***level 3***) of the maturity model, which is considered not effective although some improvements have been made. Specifically, the Department's controls over the corrective action plan process, information security architecture integration with the supply chain strategy, IT inventory reporting, and contract IT security clause administration needed improvement. These improvements

[5] The FY 2021 IG metrics include a new Supply Chain Risk Management domain within the Identify function area. However, since the new domain references SCRM criteria in NIST Special Publication (SP) 800-53, Revision 5, to provide agencies with sufficient time to fully implement it, the new metric should not be considered for the purposes of the Identify framework function rating. OIG did not rely on the SCRM by itself to determine the score for the Identify function, but rather included it for informational purposes only.

are needed because the Department's remediation and inventory processes were primarily manual efforts.

Progress Made in FY 2021

We found the Department took several actions to improve its risk management posture as follows:

Areas Improved	Actions Taken
Policies and Procedures	Established and updated its policies and procedures consistent with NIST standards; defined, communicated, and implemented policies and procedures for conducting system level risk assessments; and updated a series of its standards designed to strengthen its risk management program (including the Standard ID.RM: Cybersecurity Risk Management Framework, dated February 10, 2021; Information Assurance Services-01: OCIO/Information Assurance Services Policy Framework Instruction—Identify, dated February 9, 2021; Standard ID.AM: System Inventory, dated February 11, 2021; the Shared Service Systems (Cloud Service Provider, External Shared Service, and External General Support Systems) Overarching Standard Operating Procedures Version 2.0, dated February 26, 2021); updated its policies, procedures, and processes for developing and maintaining a comprehensive and accurate inventory of its information systems and system interconnections.
Roles, Responsibilities, and Communications	Defined and communicated across the organization the roles and responsibilities of risk management stakeholders and conducted workshops and forums to inform stakeholders to address the risk management issues. Updated a process for using standard data elements or taxonomy to develop and maintain an up-to-date inventory of hardware and software assets connected to the organization's network with the detailed information necessary for tracking and reporting.
Cyber Security Assessment and Management (CSAM) and System Security	Utilized Cybersecurity Framework Scorecard, Plan of Action and Milestones (POA&Ms) trending reports, and consolidated The Most Valuable Progress list. Enhanced the dashboard for Cybersecurity Framework domains at the enterprise level. Enabled the Microsoft Office 365 Security and Compliance Dashboard to provide in near real-time email security monitoring.

Areas Improved	Actions Taken
Enterprise-Wide Solutions	Consistently implemented its policies, procedures, and processes for system categorization, review, and communication, including the High Value Assets. Defined and communicated the policies, procedures and processes it utilizes to manage the cybersecurity risks associated with operating and maintaining its information systems. The Department consistently implemented its security architecture across the enterprise, business process, and system levels. Also, system security engineering principles are followed and include assessing the impacts to the organization's information security architecture prior to introducing information system changes into the organization's environment. Furthermore, it consistently utilizes POA&Ms to effectively mitigate security weaknesses, uses risk profiles and dynamic reporting mechanisms, and incorporates cyber risk information into the enterprise risk management program to provide a fully integrated, enterprise-wide view of organizational risks and to drive strategic and business decisions. Identified and defined its requirements for an automated solution that provides a centralized, enterprise-wide view of risks across the organization.

However, the Department's practices in all 10 metric questions still did not meet the Managed and Measurable level (***level 4***) of maturity or an effective level of security. The Department would need to achieve a Managed and Measurable level of security for at least 6 of the 10 metric questions to achieve an effective Risk Management metric domain. For example, the Department would need to ensure that the information systems included in its inventory are subject to the monitoring processes defined within the organization's Information Security Continuous Monitoring (ISCM) strategy.

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

The Department's Risk Management program remained consistent with the Consistently Implemented level of the maturity model because the Department did not implement prior years OIG recommendations, and similar conditions still existed during our FY 2021 FISMA testing.

We found that for the Risk Management metric domain, the Department was at the Optimized level (***level 5***) for one metric question, the Consistently Implemented level (***level 3***) for six metric questions, and the Defined level (***level 2***) for three metric questions. We also found that corrective action plans for recommendations from previously reported findings were not implemented at the close of our audit fieldwork. An ineffective risk management program limits the Department's ability to establish a well working 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 FY 2020 open recommendations include:

- **Recommendation 1.1**. To establish oversight controls to ensure that POA&Ms are assigned with the required criticality impact levels and remediation is conducted within the required timeframes.

- **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 1.5**. To verify and periodically reconcile the accuracy of cloud service provider inventories in or against the CSAM solution.

These recommendations were reported in the FY 2020 FISMA audit report and are scheduled to be implemented by September 30, 2021 (Recommendation 1.1 and 1.5), and September 30, 2022 (Recommendation 1.4), respectively.

Recommendations

There are no new recommendations for the *Risk Management* metric domain for this report.

METRIC DOMAIN 2—SUPPLY CHAIN RISK MANAGEMENT [*NEW*]

The new Supply Chain Risk Management (SCRM) domain focuses on the maturity of agency SCRM 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 SCRM requirements.

In previous FISMA reporting, SCRM was included as part of the Risk Management metric domain. For the FY 2021 IG FISMA Metrics, supply chain risk management was assigned its own metric domain area. However, for FY 2021 reporting, the SCRM metric domain will not be considered in the determination of the Identify framework function rating and is included only ***for informational purposes***.

Progress Made in FY 2021

We found the Department took the following actions to improve its supply chain risk management posture as follows:

Areas Improved	Actions Taken
Policies and Procedures and Processes	Defined and communicated a series of policies and procedures including the organization wide SCRM strategy, Information and Communications Technology SCRM Roadmap and Plan, Standard ID.SC: Information and Communications Technology SCRM, and Information and Communications Technology Supply Chain Deep Dive Risk Assessment Methodology.
Products, System and Components	Defined and communicated policies and procedures to ensure that organizationally defined products, system components, systems, and services adhere to its cybersecurity and supply chain risk management requirements. It also established a Memorandum of Understanding with the Department of Energy for operational SCRM program and will utilize its services for High Value Assets.

However, the Department's practices in all four of its metric questions still did not meet the Managed and Measurable level (***level 4***) of maturity and an effective level of security. The Department would need to achieve a Managed and Measurable level of security for at least three of the four metric questions to achieve an effective SCRM metric domain rating. For example, the Department would need to ensure that it monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its SCRM strategy and makes updates, as appropriate.

Finding 2. The Department's Supply Chain Risk Management Program Needs Improvement

We found that for the SCRM metric domain, the Department was at the Defined level (***level 2***) for three metric questions and the Ad Hoc level (***level 1***) for one metric question. During our fieldwork, the Department was subject to and relied on NIST 800-53, Revision 4. The new criteria, NIST SP 800-53, Revision 5, with SCRM, as a separate metric, will not go into effect until September 2021. As a result, we did not identify specific findings for the SCRM metric domain for FY 2021.

However, corrective action plans for prior findings within the Risk Management metric that included SCRM recommendations were not implemented at the close of our audit fieldwork. The following open recommendations on Risk Management from the FY 2020 FISMA audit report on SCRM are scheduled for implementation by September 30, 2021:

- **Recommendation 1.2**. To develop and implement 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.

- **Recommendation 1.3.** To develop a process to evaluate and routinely monitor supply chain risks associated with the development, acquisition, maintenance, and disposal of systems and products.

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.

Recommendations

The recommendations for this area are scheduled for implementation by September 30, 2021; therefore, we are not making any new recommendations for FY 2021.

SECURITY FUNCTION 2—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 Consistency Implemented level (***level 3***) of the maturity model.

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 Consistently Implemented level (***level 3***) of the maturity model, although some progress has been made. The Department remains at this level because it continues to rely on unsupported operating systems, applications, and weak encryption protocols. The Department was not enforcing its vulnerability and patch management policies and standards, didn't adequately safeguard the personally identifiable information (PII) data, and had insufficient controls over web applications and servers.

Progress Made in FY 2021

We found the Department took several actions to improve its configuration management posture as follows:

Areas Improved	Actions Taken
Policies and Procedures and Processes	Executed policy that requires the use of the Federal Risk and Authorization Management Program for new cloud service providers prior to authorizing cloud service providers on the Department and FSA network(s); improved effectiveness of security controls; fully authorized the change management process; implemented ServiceNow as a tracking mechanism; automized monitoring of in near real-time configuration changes; implemented continuous monitoring on vendors via automated feeds to FSA, Next Generation Data Center, and FSA Cloud; implemented monitoring capabilities on a real time basis; and enforced the system owners accountability via the Cybersecurity Framework Risk scorecard.

Areas Improved	Actions Taken
Baseline Configurations and Collaboration Efforts	Enhanced phishing reporting capabilities with a quick reporting button to report potential suspected phishing emails; incorporated warning banners for external e-mails; automated change management process; established baseline standards for the Department's Chief Information Security Officer; enforced the lessons learned from past incidents; integrated the security with the lifecycle processes; deployed automated mechanisms; improved the network access control solution; enhanced Endpoint capabilities protections; enhanced the application whitelisting and automated tools or techniques used to detect unauthorized hardware, software, or firmware on its network; enabled Endpoint capabilities protection for its systems; and improved its collaboration efforts by working with the Department of Homeland Security and other agencies during mitigating of SolarWinds, FireEye, and Malwarebytes cyber-attack.
Patch Management	Enhanced patching of a zero-day exploits as part of the patch management process, enhanced escalation, and monitoring processes.
Trusted Internet Connections and Network Access Control Solutions	Developed and defined plans for meeting the goals of the Trusted Internet Connection initiative, including Trusted Internet Connection 1.0, 2.0, and 3.0. Enhanced its inventory processes for external connections by meeting the defined Trusted Internet Connection security controls and routing all agency traffic through defined access points.
Vulnerability Disclosure	Defined the collaboration between Federal agencies and vulnerability researchers who are members of the public.

However, the Department's practices in six of the eight metric questions still did not meet the Managed and Measurable level (***level 4***) of maturity or an effective level of security. The Department would need to achieve a Managed and Measurable level of security for at least five of the eight metric questions to achieve an effective Configuration Management metric domain. For example, the Department would need to ensure that it monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of flaw remediation processes and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.

Finding 3. The Department's Configuration Management Program Needs Improvement

We found that for the Configuration Management metric domain, the Department was at the Managed and Measurable level for two metric questions, the Consistently Implemented level for three metric questions, and the Defined level for three metric questions. We determined the Department and FSA's controls needed improvement for

relying on vendor-supported operating systems in its production environment; using appropriate application connection protocols; consistently performing system patching; protecting PII; consistently using secure connections; and improving controls over web applications and servers.

These conditions occurred because the Department continues to rely on weak encryption protocols and unsupported operating systems and applications. Furthermore, the Department did not consistently implement controls for enforcing its vulnerability and patch management policies and standards and didn't safeguard PII data in its systems. An ineffective configuration management program limits the Department's ability to establish and maintain consistent and secure performance of system resources, computer systems, servers, and other assets.

The Department and FSA Relied on Unsupported Applications and Operating Systems in its Production Environment

We found that the Department and FSA continued to rely on applications and operating systems that were no longer supported by its vendors. We analyzed Department-provided network scans and conducted our own scans of FSA systems. We reviewed 70 different network vulnerability scan results and identified a total of 223 obsolete applications and operation systems. Continued reliance on the obsolete systems or applications could potentially make these applications and operating systems vulnerable to intentional and unintentional compromises. Further, relying on unsupported applications and operating systems could lead to data leakage and exposure of PII that can further compromise the Department's integrity and its reputation. Systems that reach their "end of life" cycle are no longer supported or patched by the vendor and could become vulnerable to new exploits such as post-retirement "zero-day" and other malicious attacks[6]. We reported similar conditions in our FY 2018, FY 2019, and FY 2020 FISMA audits.

The Department and FSA Continue to Run Outdated Protocols on Its Websites

We found that the Department and FSA have not fully disabled and discontinued use of outdated secure connection protocols. In response to our FY 2020 FISMA report the Department stated that it would develop a corrective action plan by December 31, 2020, to address the continued use of outdated protocols. The Department's continuous oversight was ineffective. Our testing on all 633 uniform resource locators provided in the Department's website master inventory validated that 4 of the 633 provided

[6] A zero-day exploit is an attack that exploits a previously unknown hardware, firmware, or software vulnerability.

websites[7] continue to use weak, vulnerable, or obsolete protocols to encrypt traffic in transit. Specifically, we identified two of the Department's websites that continue to rely on the Transport Layer Security (TLS) 1.0 protocol, which was deprecated in October 2018 and no longer supported. We also identified two additional websites that continue to rely on the TLS 1.1 to encrypt data on Department servers. Although TLS 1.1 is not prohibited by NIST, it is not supported by the Cisco Umbrella Services and industry services.

In addition to our testing, we reviewed Department provided scan results and identified that the following outdated protocols were in use:

- 28 systems using TLS 1.0,
- 8 systems using TLS 1.1,
- 1 system using Secure Socket Layer (SSL) 2.0, and
- 21 systems using SSL 3.0.

NIST and commercial industry leaders have recommended the discontinued use of Secure Socket Layer Version 3 protocol and below. However, the Department and FSA continued to rely on outdated protocols to encrypt its traffic in transit.

The Department and FSA need to take steps to provide assurance that obsolete encryption algorithms—such as TLS 1.0 and TLS 1.1—are no longer enabled as an option to encrypt. We reported a similar condition in our FY 2018, FY 2019, and FY 2020 FISMA audits. These conditions have not been addressed due to insufficient monitoring and controls over configurations. The Department stated that it would have a corrective action plan in place by December 31, 2020. However, the plan has not been effective, and these outdated protocols should not be in use.

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 TLS 1.2 and begin to transition to TLS 1.3 on or before January 1, 2024. These servers should not be configured to use TLS 1.1 and shall

[7] Inventory included various domains, including the .com, .gov, .org, .net, and .us addresses managed or overseen by the Department.

not use TLS 1.0, SSL 3.0, or SSL 2.0[8]. However, the Department and FSA have not disabled the option to use weak encryption protocols, such as SSL, TLS 1.0, or TLS 1.1. 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.

Patches Were Not Being Applied Within the Required Timeframes

We found that the Department did not consistently apply software patches and the latest security updates to its systems and solutions within required timeframes. In response to our FY20 FISMA report, the Department stated that it would develop a corrective action plan by December 31, 2020, to enhance vulnerability management controls. The Department's patch management was not adequate. The Department was conducting scans but didn't have a process in place to review results and take timely actions. To test the Department's compliance with applying patches, OIG obtained and examined the most recent 70 vulnerability scan results. 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 127 missing patches with a criticality designation of medium or higher (9 critical, 31 high, and 87 mediums). For example, our review of a network vulnerability scan results dated May 15, 2021, disclosed two critical vulnerabilities; one was initially detected on November 15, 2018, and should have been resolved within 15 days. However as of May 2021, it was still unresolved. Another vulnerability was identified on February 12, 2021, and remained open as of May 15, 2021.[9]

Department policy, *Vulnerability Management Standard Operating Procedure*, dated April 12, 2021, driven by the criticality level, 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. OIG identified over 100 patches that should have been mitigated. The Department did not consistently implement and lacked proper controls for enforcing its vulnerability and patch management policies and

[8] NIST SP 800-52, Revision 2, "Guidelines for TLS Implementations," states that Protocol Version Support Servers supporting government-only applications shall be configured to use TLS 1.2 and should be configured to use TLS 1.3 as well. These servers should not be configured to use TLS 1.1 and shall not use TLS 1.0, SSL 3.0, or SSL 2.0. TLS versions 1.2 and 1.3 are represented by major and minor number tuples (3, 3) and (3, 4), respectively, and may appear in that format during configuration.

[9] OIG did not verify subsequent scans to verify whether the vulnerability was patched.

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, and FY 2020 FISMA audits.

Personally Identifiable Information Was Not Being Adequately Protected

The Department and FSA didn't ensure that all websites masked PII (primarily Social Security numbers and dates of birth) entered by users to create accounts. During our review of the 633 websites, we identified 3 websites that require users to provide a Social Security number, with 2 also requiring a date of birth to create an account. We verified that these websites were not configured to mask this information and displayed the information in plain text as it was entered.

We found that the Department and FSA did not consistently implement appropriate controls to safeguard the security, integrity, and confidentiality of records and enforce the protection of PII. According to OMB-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual. These data elements include Social Security numbers and other identifiers. The OMB is also clear that agency shall consider Security Safeguards, including encryption, redaction, data masking, and remote wiping. If the Department continues to request users to enter PII that is not being adequately protected during creation of user accounts, it risks subjecting individuals' information to compromise from malicious attacks, such as keylogging, screen scrapes, or shoulder-surfing, resulting in identity theft.

Department Did Not Consistently Ensure the Use of Secure Connections

In 2015, the OMB provided guidance to Agencies to migrate all websites from Hypertext Transfer Protocols (HTTP) to HTTP Secure (HTTPS) encryption protocol. We found that the Department did not enable this protocol on its websites to protect users and their information submitted through web portals. Specifically, our testing found that 9 of the 633 websites we tested used weak and non-compliant HTTP as a default connection. OMB M-15-13, *Policy to Require Secure Connections Across Federal Websites and Web Services*, requires that all publicly accessible Federal websites and web services provide service only through a secure connection. Further, agencies were required to make all existing websites and services accessible through a secure connection (HTTPS-only, with HTTPS Strict Transport Security (HSTS)) by December 31, 2016[10]. Compromising a user account could allow a malicious actor to use those compromised credentials to further

[10] HTTP is the foundation of data communication for the World Wide Web. HSTS allows web servers to declare that web browsers should only interact with it using secure HTTPS connections.

exploit the user, which could be used to conduct malicious activities and possibility lead to identity theft. Failure to encrypt traffic could result in man-in-the-middle attacks or other attacks where unencrypted data in transit could be intercepted by a malicious user or packet grabbing tools. We reported a similar condition in FY 2018, FY 2019, and FY 2020 FISMA audits.

FSA's Controls over Web Applications and Servers Were Insufficient

OIG continues to identify FSA's application security controls that were not fully implemented or enforced. FSA web application vulnerabilities increase the risk of unauthorized access to critical security architecture. We assessed web application security for three of the five systems selected for testing. We also conducted network testing on the other two systems to conduct a comprehensive analysis from both an internal and external perspective. We found that some key security controls were effectively implemented (such as data validation, secure coding, and web security). However, there were key external controls that were not in place to secure FSA's application posture, including those in the internal network. We identified instances of

- reflected cross-site scripting,[11]
- outdated operating systems,
- missing operating system and third-party security patches, and
- unnecessary or malicious services enabled on internal systems.

We determined that the Department did not implement controls to enforce adequate system configuration practices. Inadequate system configuration practices increase the potential for unauthorized activities to occur without being detected and could lead to potential theft, destruction, or misuse of Department data and resources.

NIST SP 800-53, Revision 4, 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 baseline configuration, unsupported system components, transmission confidentiality and integrity, vulnerability scanning, authenticator management, and patch management.

[11] A malicious user can access any cookies, session tokens, or other sensitive information retained by the browser and use it to gain unauthorized access to the account or steal usernames, passwords, sensitive data, etc.

Recommendations

We recommend that the Chief Information Officer require OCIO to—

3.1 Take steps to assure obsolete solutions and encryption protocols are either updated, removed, or replaced.

3.2 Implement additional measures for patches to be applied in a timely manner based on a priority basis.

3.3 Ensure all Department websites are configured to mask PII when used as an identifier.

3.4 Enforce secure connections as required by OMB M-15-13 for all existing websites and services.

3.5 Require FSA to take immediate corrective actions to mitigate the vulnerabilities identified during the vulnerability assessment.

Department Comments

The Department agreed with Recommendations 3.1, 3.2, 3.3, 3.4, and 3.5, and committed to address these recommendations by December 31, 2021.

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 2022 FISMA audit.

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 resources. 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 Defined level (***level 2***) of the maturity model, although some improvements have been made. The Department remained at this level because oversight controls were not in place and operating. Specifically, the Department's ICAM strategy was not fully implemented, the 30-minute timeouts did not function as intended, the risk position designations were not properly documented, the Department's strong authentication and banners were not consistently enforced, the

endpoint security safeguards were not sufficient, and FSA's controls over database management were not secured.

Progress Made in FY 2021

We found the Department took several actions to improve its identity and access management posture as follows:

Areas Improved	Actions Taken
Policies and Procedures	Developed a comprehensive Identity, Credential, and Access Management (ICAM) strategy, process, and technology solution road map to guide its ICAM processes and activities and developed milestones for how it plans to align with Federal initiatives, including strong authentication, the Federal ICAM architecture and OMB M-19-17, and phase 2 of the Department of Homeland Security's Continuous Diagnostics and Mitigation program.
Roles and Responsibilities	Defined and communicated roles and responsibilities at the enterprise and information system levels for stakeholders involved in the ICAM program, established a process to hold stakeholders accountable for carrying out their roles and responsibilities effectively, and defined and communicated its process for ensuring that all personnel are assigned risk designations and appropriately screened prior to being granted access to its systems.
Access Agreements	Ensured that access agreements for individuals are completed prior to being granted access to systems and are consistently maintained thereafter and required continuous role-based training for privileged users.
Strong Authentication	Implemented strong authentication mechanisms for non-privileged users of the organization's facilities and networks, including those with remote access, in accordance with Federal targets.
Enterprise ICAM solution	Implemented an integrated, agency-wide ICAM team in support of its Enterprise Risk Management capability to effectively govern and enforce ICAM efforts, and allocated its resources in a risk-based manner to effectively implement identity, credential, and access management activities.

However, the Department's practices in all eight of its metric questions still did not meet the Managed and Measurable level (***level 4***) of maturity or an effective level of security. The Department would need to achieve a Managed and Measurable level of security for at least five of the eight metric questions to be considered effective. For example, the Department would need to ensure that it integrates its ICAM strategy and activities with its enterprise architecture and the Federal ICAM architecture.

Finding 4. The Department's Identity and Access Management Program Needs Improvement

We found that for the Identity and Access Management metric domain, the Department was at the Managed and Measurable level for one metric question and the Defined level for seven metric questions. We determined the Department and FSA's controls needed improvement for implementing an ICAM strategy—disconnecting users after 30 minutes of inactivity, documenting risk position designations, implementing strong user authentication recertifying user access, configuring website warning banners, and database management. These conditions occurred because the Department's ICAM strategy was not fully implemented, the 30-minute timeouts did not function as intended, the risk position designations were not properly documented, and the Department's strong authentication and banners were not consistently enforced. 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.

ICAM Strategy Has Not Been Fully Implemented

The Department continues to make progress in implementing a multi-year ICAM strategy to deploy an enterprise-wide solution. Overall, the Department has defined and incorporated Digital Identity Risk Management into existing Department processes and assessed an Identify and Authenticator Assurance Level for its systems. In addition, the Department developed milestones to align with the Federal ICAM architecture, OMB M-19-17 *Enabling Mission Delivery Through Improved Identity, Credential, and Access Management* and Phase 2 of the Department of Homeland Security's Continuous Diagnostics and Mitigation program.

ICAM is the set of tools, policies, and systems that an agency uses to enable the right individual to access the right resource, at the right time, for the right reason in support of Federal business objectives. The Department relies on ICAM to support its practices to accomplish and remain within the framework of the Federal ICAM architecture. The Department defined an ICAM strategy to ensure they meet established ICAM implementation dates. However, we found the Department either has not met or was not on track for completion of its established milestone dates as of July 2, 2021. In addition, Phase 2 of the Continuous Diagnostics and Mitigation Program requirements have not been fully integrated into ICAM. Without full implementation of the ICAM strategy, the Department cannot ensure full accountability of access management to Department systems, especially those hosted externally. The Department's inventory of FISMA-reportable systems accounted for 119 systems, of which 99 are contractor systems and 20 are Federal Risk and Authorization Management Program cloud service

providers. In addition, 11 of the 119 systems are considered High Value Asset systems.[12] Even though all these systems directly supported mission-essential functions, only 17 had been registered for integration into ICAM.

Virtual Private Network Connections Didn't Disconnect After 30 Minutes of User Inactivity

We found that FSA's Next Generation Data Center's virtual private network connection session expiration does not function as intended. Our testing disclosed that FSA's Next Generation Data Center's virtual private network connections did not terminate user sessions after 30 minutes of inactivity. The 30-minute timeout is to limit the exposure of session-based attacks by disconnecting an inactive user on the virtual private network connection. However, the FSA Next Generation Data Center's virtual private connection not only failed to terminate our test user session after 30 minutes of inactivity, but also did not require reauthentication after the required 12 hours of an extended usage session. Furthermore, when our user machine was reactivated and restored from sleep-mode, our tester was able to restore the session without being prompted to reauthenticate.

NIST SP 800-63B, *Digital Identities Guidelines*, states that reauthentication of a user shall be repeated following any period of inactivity lasting 30 minutes or longer, or at least once per 12 hours during an extended usage session, regardless of user activity, at which point the session shall be terminated (i.e., logged out). Failure to properly disconnect users could allow a user who has gained unauthorized access to remain on the network for an extended period. In addition, the lack of time-out restrictions could allow a user to reconnect (from sleep-mode) without the need to reauthenticate and gain access to network resources via a prior established authorized connection.

Risk Position Designations Not Properly Documented

The Department did not consistently document position risk designations for background investigations. We judgmentally selected 22 users (10 privileged users and 12 non-privileged users) and requested the Risk Position Designation Form for each user. The Department was not able to provide a Risk Position Designation Form for two privileged and six non-privileged users. We determined that Risk Position Designation Forms are not managed and tracked in a centralized location to ensure evidence of accurate assignment of position sensitivity level. NIST SP 800-53, Revision 4, specifies security controls for organization and information systems supporting the executive

[12] A High Value Asset is information or an information system that is so critical to an organization that the loss or corruption of this information or loss of access to the system would have serious impact to the organization's ability to perform its mission or conduct business.

agencies of the Federal government to meet the requirements of Federal Information Processing Standards Publication 200, *Minimum Security Requirement for Federal Information Systems* that includes account management and access agreements. Without evidence that the Office of Personnel Management's Position Designation Tool is utilized and maintained for assessing employee or contractor position sensitivity level, there is an increased risk positions will not be properly designated based on risk and national security position duty requirements.

Strong User Authentication Mechanisms Not Consistently Applied

We found that FSA did not consistently enforce configuration for the use of two-factor authentication. For 633 FSA websites identified, we used the Uniform Resource Locator Profiler tool to assess the security posture and determine whether websites complied with Federal guidance. Our testing found that of the 633 websites, 31 were not configured to use two-factor authentication. We identified three privileged users with access to Department critical resources with a personal identity verification exemption resulting in the Department not complying with its Privileged User Access Standard Operating Procedure requirement that privileged users must have a personal identity verification card to access Departmental systems. We further noted that the increased number of recent hires in the current pandemic working conditions resulted in a net increase of 630 users that do not utilize a personal identity verification card to authenticate to the network. As a result of the increase, the Department did not meet their target of 85 percent of all users issued a personal identity verification card. The increase of new users reduced the Department's target below the 85 percent to 80 percent of new users are issued a personal identity verification card. Because of the physical logistic limitations to Departmental badging locations, users were not able to obtain a personal identity verification card. Users who lacked a valid personal identity verification card were temporarily authorized access to the Department's network and information systems through an alternative multi-factor authentication solution.

NIST SP 800-53, Revision 4, specifies 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* that includes access control, identification, and authentication; account management; and remote access. On August 27, 2004, the President signed Homeland Security Presidential Directive-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, which requires the development and implementation of a mandatory, government-wide standard for secure and reliable forms of identification for Federal employees and contractors. Failure to implement two-factor authentication will allow a user with a username and password to remotely connect and access network resources.

Recertification of User Access Was Not Consistently Performed

System user accounts (both privileged and non-privileged) must undergo regularly scheduled reviews to recertify and maintain each Department system's validity. Evidence that the recertification of system user accounts has occurred is signed by the Information Security Officer or Information System Security Officer and documented in CSAM under the AC-02 control.

We reviewed five systems to ensure that the recertification was performed for privileged and non-privileged users and documented in CSAM. We did not find evidence that the recertification of user accounts was performed for four of the five systems. Three of these four systems are designated as high-value assets and are required to recertify privileged user accounts monthly. Also, for three of five systems, we did not see evidence in CSAM that user recertifications for non-privileged users were documented. In addition, during our review, we identified one user who had been terminated by the Department 2 years earlier, yet still had access to the Department's training system. Stakeholders with responsibilities to ensure recertification reviews are performed based on system type and sensitivity level did not consistently or accurately account for the evidence of recertification for privileged users and non-privileged users.

The Department Cybersecurity Protect Core Instruction falls within the scope of the overarching Department of Education, OCIO-3-112 Cybersecurity policy. Within each function, Department Standards provide further guidance on cybersecurity practices. Education Standard PR.AC User Account Recertification Standard, February 11, 2021, requires that Information Security Officers must conduct regular recertification reviews of user accounts based on system type and sensitivity level and service accounts based on mission or business need, according to the required frequencies of review as described within this standard. Information System Security Officers must confirm and certify that user account recertification reviews have occurred at the required frequencies for system type and sensitivity level. Without recertification reviews performed as required, there is an increased risk that users will not be removed from Departmental resources which will result in users with excessive access to critical Departmental resources.

Websites Were Not Configured to Display Warning Banners

We used the Uniform Resource Locator Tool to verify if websites complied with Federal guidance requiring websites to display user notification or system warning banners and found that 49 of 633 FSA websites did not display user notifications or system warning banners. The Department communicated to its stakeholders, including FSA, that banners and acceptable text are required to be in place by October 1, 2018. In the Department's corrective action plan for the FY 2018 FISMA audit, the Department planned to finish configuring all websites to display warning banners by October 31, 2019. Further, a corrective action plan to document and implement a user

notification or system warning banner prior to issuing an Authority to Operate was closed in June 2021. As part of this corrective action, the Information Security Officer and Information System Security Officer are required to ensure the Department's standard system use notification or warning banner is documented and implemented through the system's security plan before an Authority to Operate is issued. Although this corrective action plan was closed, we found that the Department was not consistently enforcing this requirement.

NIST SP 800-53, Revision 4, provides guidelines for selecting and specifying security controls for organization and information systems supporting the executive agencies of the Federal government that includes system use notification—requiring that organizations display to users a notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable Federal laws. Failure to display a banner with a warning label that outlines user expectations could lead to individuals accessing and misusing government resources. We reported a similar condition in our FY 2018, FY 2019, and FY 2020 FISMA audits.

The Department's Endpoint Security Safeguards Were Not Sufficient

Department and FSA controls over their own configuration and security settings were not consistently enforced or properly protected. As part of our security assessment testing, OIG executed an adversarial testing scenario to simulate an insider threat attack. This exercise was conducted in coordination with Department and FSA Officials with a need-to-know basis.

Our testing team was provided with an authorized standard FSA user account, government-furnished laptops, and virtual private network accounts to conduct their tests. The team also initiated a spear phishing campaign. The team had positive results on the tests of the technical security controls and architecture supporting the infrastructure. The spear phishing attack was successfully handled by the Department. However, the team discovered vulnerabilities with high severity with the government-furnished laptops. Due to the sensitivity of the vulnerabilities, we have disclosed the items separately to the Department and FSA for review and remediation.

NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems,* states that Federal agencies are responsible for compliance with minimally acceptable system configuration requirements, as determined by the agency within their information security program. It further elaborates that managing system configurations are also a minimum-security requirement identified in Federal Information Processing Standards 200, 3 and NIST SP 800-53, Rev 4, which defined the controls that support this requirement.

The Department had not implemented sufficient oversight controls to ensure its endpoint protections were in place and functioning as intended. Failure to implement safeguards to protect end-user machines such as workstations and laptops against attack (e.g., antivirus, antispyware, anti-adware, personal firewalls, and host-based intrusion detection and prevention systems) could result in a breach and cause damage to the Department reputation.

FSA's Controls Over Database Management Were Not Secured

We performed assessments that identified vulnerabilities, configuration errors, and access issues for databases included in three of the five systems reviewed—Access & Identity Management Service (AIMS), Person Authentication Service, and Financial Management Service (FMS). Specifically, the vulnerability scans identified significant security weaknesses that FSA needs to address to better safeguard data stored in its databases. Scans of databases associated with these systems identified

- 21 high vulnerabilities: 6 High (FMS) and 15 High (AIMS)
- 95 medium vulnerabilities: 35 Medium (FMS) and 60 Medium (AIMS)
- 55 low vulnerabilities: 16 Low (FMS) and 39 Low (AIMS)

Specifically, we found that

- security parameters were not correctly set;
- permissions, privileges, and roles were incorrectly assigned;
- configurations were improper;
- failed login attempt and password parameters were incorrectly set; and
- audit data records were not encrypted.

FSA had not consistently implemented the necessary controls to ensure that its databases were protected. We shared the vulnerabilities with FSA for remediation.

NIST SP 800-53, Revision 4, 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 FISMA audits.

Recommendations

We recommend that the Chief Information Officer require OCIO to—

4.1 Fully implement ICAM Strategy by established milestones to ensure the Department meets full Federal government implementation of ICAM.

4.2 Take steps to ensure user activity is terminated on the FSA Next Generation Data Center after 30 minutes.

4.3 Document and maintain position risk designation forms for background investigations.

4.4 Enforce a two-factor authentication configuration for all user connections to systems and applications.

4.5 Perform and evidence regularly scheduled reviews of system user accounts (both privileged and non-privileged) to recertify and maintain each Department system's validity.

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

4.7 Identify and enforce all websites to display warning banners when users login to Departmental resources.

4.8 Take immediate corrective actions to mitigate the vulnerabilities identified during the endpoint vulnerability assessment.

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

Department Comments

The Department agreed with Recommendations 4.1, 4.2, 4.3, 4.5, 4.6, 4.8, and 4.9, and partially agreed with recommendations 4.4 and 4.7. For recommendation 4.4, it stated that it must have the ability to have exemptions and that not all systems or users are required to have multi-factor authentication based on the type of information the systems share or the type of data that is used or stored by the system. At the same time, the Department will continue to ensure that all relevant systems meet this requirement in FY 2022 and will develop a corrective action plan by December 31, 2021.

Likewise, for recommendation 4.7, the Department stated that it must have the ability to have exemptions and that not all websites are required to have warning banners. The Department will continue to ensure that all applicable websites have warning banners in FY 2022 and will develop a corrective action plan by December 31, 2021.

OIG Response

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 2022 FISMA audit.

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 including any information 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 Defined level (***level 2***) of the maturity model, although some improvements have been made. Improvements are needed for this program because the Department's process for validating required privacy documentation for Privacy Impact Assessments (PIA) and System of Records Notices (SORN), was not fully implemented or consistently enforced. 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 2021

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.

Areas Improved	Actions Taken
Policies and Procedures	Defined and communicated its privacy program plan and related policies and procedures for the protection of PII, data exfiltration, and its Data Breach Response Plan, including its processes and procedures for data breach notification; defined and communicated its privacy awareness training program, including requirements for role-based privacy awareness training; in February 2021, updated the "Standard ID.RM: Cybersecurity Risk Management Framework" with details for privacy significance in the Risk Management Framework and articulates the role of the Senior Agency Official for Privacy (SAOP) in the Department's Cybersecurity Risk Management Framework; and in January 2021, the Secretary signed a new Disclosure Review Board charter and a new process has been established to better assess proposed disclosures.
Roles and Responsibilities	Roles and responsibilities for the effective implementation of the organization's privacy program have been defined; a permanent SAOP was hired to lead the Student Privacy Policy Office, which contains the Department Privacy Program Office; and the Student Privacy Policy Office team is now an active participant in the Department's Authority to Operate approval process, the incident response team, the Privacy Threshold Analysis and PIA process, and the Cybersecurity Framework Risk Scorecard.
Data Protection Security Controls and Enhancements	Used effective communications channels for disseminating privacy policies and procedures; used Federal Information Processing Standards-validated encryption of PII and other sensitive data, as appropriate, both at rest and in transit; ensured removeable media policies, processes and procedures are consistently implemented on PIVOT-I endpoints; consistently monitored inbound and outbound network traffic, ensuring that all traffic passes through a web content filter that protects against phishing, malware, and blocks against known malicious sites; and ensured that all individuals receive basic privacy awareness training and individuals having responsibilities for PII or activities involving PII receive role-based privacy training at least annually.

However, the Department's practices in all five 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 three of the five metric questions to achieve an effective rating. For example, the Department would need to develop and implement an effective quality control review process to help ensure that PIAs and SORNs were up to date and complete.

Finding 5. 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 four metric questions. We determined the Department and FSA's controls needed improvement for documenting PIAs and SORNs and documenting the sanitization of digital media.

The Department Did Not Consistently Document Privacy Impact Assessments and System of Records Notices

The Department was not consistently documenting PIAs and SORNs. We judgmentally selected five systems and determined that the

- Department did not update a PIA for one system after the system migrated to a new cloud environment, which posed new privacy risks as a significant system management change;
- SORN reference included in the Department's CSAM tool for one system was outdated and not linked to the current SORN; and
- SORNs for three systems were not updated to reflect major changes to the systems (data center migration to a cloud environment).

We confirmed that the Department is still in the process of addressing an open recommendation from the FY 2020 FISMA audit that identified a similar deficiency. The recommendation has a planned completion date of September 30, 2021. Although the Department established a process for the completion and maintenance of PIAs and SORNs, it still has not formally developed or implemented an effective quality control review process to help ensure that PIAs and SORNs were up to date and complete. In addition, as part of the FY 2020 SAOP FISMA metrics submission, the Department self-reported that only 41 out of a total of 103 SORNs were up to date and have published in the Federal Register. Also included in the submission, the Department stated that it was aware that many of its SORNs are older and do not contain all the information required by OMB, and it was working to update them. However, the Department has lacked the capacity to execute the planned fixes to the SORNs.

Administrative Communications System Departmental Directive OM: 6-108, *Privacy: Section 208 of the E-Government Act of 2002 Policy and Compliance*, states that PIAs are reviewed whenever a system change creates new privacy risks and at least every 2 years for systems or programs for which they are responsible and update as needed. Also, the Department must update PIAs when a system change creates new privacy risks. Administrative Communications System Departmental Directive OM:6-104, *The Privacy Act of 1974 (The Collection, Use, and Protection of Personally Identifiable Information)*,

Significant Alteration of a System of Records, states that the significant alteration of an existing system of records requires an altered system notice and a system report. By not consistently documenting, validating, and maintaining PIAs and SORNs as required, the Department cannot ensure that systems reflect the most current privacy risks. Without an effective monitoring process in place, there is limited assurance that the PIAs and SORNs are accurate and valid.

Although we did identify similar findings for the *Data Protection and Privacy* metric domain for FY 2021, we found that corrective action plans for recommendations from previously reported findings were not implemented at the close of our audit fieldwork. As a result, we are not making new recommendations until the open recommendations from prior FISMA reports are closed out. However, If the Department effectively addresses Recommendation 4.1 from the FY 2020 FISMA audit (A11U0001), then this deficiency should be resolved:

- **Recommendation 4.1**. To establish additional processes, procedures, and monitoring controls to validate, track and enforce the completion of PIAs, Privacy Threshold Analyses PTAs, and SORNs**.**

This recommendation was reported in the FY 2020 FISMA audit report and is scheduled to be implemented by September 30, 2021.

Documentation Not Complete Supporting Sanitization of Digital Media

According to Department officials, Information System Owners are required to comply with NIST Special Publication SP 800-53, Revision 4, Control MP-6 and 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. Furthermore, according to Department officials, when an employee or contractor is terminated, an offboarding request is submitted via ServiceNow.[13] As part of the process, the end user is sent a box with a return mailing label to return their device(s) (or PIVOT-I endpoint) back to the Department's PIVOT-I contractor. The contractor wipes, then reimages the device(s) for redeployment to another Departmental user. All these activities are tracked and maintained in ServiceNow.

PIVOT-I systems are designated as security categorization Moderate. According to the Department's Media Sanitization Standard Operating Procedure, PIVOT-I-IT-SM-PRO24,

[13] 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.

per NIST 800-88 guidance, Clear Sanitizing is applied on all reused PIVOT-I endpoints and the asset life-cycle information is documented within the ServiceNow Configuration Management module.[14]

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. We judgmentally selected a sample of 10 out of 479 employees or contractors from the Department's provided list of offboarded or soon to be offboarded employees from October 1, 2020, through March 4, 2021. We requested the Department to provide detailed evidence of digital media sanitization for all devices used by the individuals. As a result, the Department did not provide adequate evidence showing the proper documentation and validating of clear sanitizing for all digital media assigned to the 10 offboarded employees or contractors. No evidence was provided showing any type of Certificate of Sanitization, or other alternate electronic record (ServiceNow Configuration Management details) showing sanitization details in accordance with Federal rules and regulations.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, states that the organization sanitizes organization-defined information system media prior to disposal, release out of organizational control, or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable Federal and organizational standards and policies. In addition, it states that the organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions. NIST SP 800-88, Revision 1, *Guidelines for Media Sanitization*, Section 4.6, states that upon completion of sanitization decision making, the organization should record the decision and ensure that a process and proper resources are in place to support these decisions. It further states that following sanitization, a certificate of media disposition should be completed for each piece of electronic media that has been sanitized.

The Department's digital media sanitization policies and processes were not adequate and not as robust as some of its other security controls surrounding the protection of PII and other agency sensitive data (for example, data encryption and removable media limitations). In addition, the written policies and procedures contained many irregularities. For example, the Media Sanitization Standard Operating Procedure (PIVOT-I-IT-SM-PRO24) was originally created in February 2018; however, the PIVOT-I contract did not begin until November 2018. In addition, the most recent update made

[14] According to NIST, clear sanitizing uses software or hardware products to overwrite user-addressable storage space on the media with non-sensitive data, using the standard read and write commands for the device.

to this document was July 1, 2021, which was over a month after we requested the specific evidence. Lastly, the Department's digital media sanitization policy is incomplete. According to the Media Sanitization Standard Operating Procedure, the Disposal (Destroy) process for devices is in a "Work In Progress" status until May 2022, and any laptop that needs to be destroyed is locked up at headquarters until the completed disposal process is created.

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.

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 SAOP to—

5.1 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.

Department Comments

The Department agreed with Recommendation 5.1 and will develop a corrective action plan by December 31, 2021.

OIG Response

OIG will examine the proposed corrective action plan to determine whether the action will address the finding and recommendation and, if so, will validate this action during our FY 2022 FISMA audit.

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.

We determined that the Department's security training program was consistent with the Consistently Implemented level (***level 3***) of the maturity model, although some progress has been made. The Department remains at this level because of its inconsistency in addressing and implementing prior audit recommendations.

Progress Made in FY 2021

We found the Department took several actions to improve its security training posture as follows:

Areas Improved	Actions Taken
Policies, Procedures, and Standards	Defined its policies and procedures for security awareness and specialized training; developed procedures for conducting phishing exercises for Department active network accounts; updated the Standard PR.AT: Cybersecurity Awareness and Training, which established the Department standard for cybersecurity awareness and role-based training; and updated its policies and procedures to incorporate any updates in the security training and implement new processes to keep the Department's systems and information secure. Furthermore, the Training Program Manager was nominated and won the Federal Information Security Educators' Cybersecurity Awareness and Training Innovator Award.
Enterprise-Wide Training Strategy	Consistently implemented the role-based training process and ensured that users with significant security responsibilities completed training and enforced its process for suspending the accounts of users who failed to take the Cybersecurity and Privacy Awareness training. Moreover, it consistently implemented its organization-wide security awareness and training strategy and plan, as well as periodically updated its assessment to account for a changing risk environment.

Areas Improved	Actions Taken
Roles and Responsibilities	Defined and communicated roles and responsibilities for security awareness and training program stakeholders across the organization, implemented the role-based training process and ensured that users with significant security responsibilities completed the training, consistently implemented a process to ensure that individuals with significant security responsibilities completed the Department's defined specialized security training, and maintained completion records for specialized training taken by individuals with significant security responsibilities.
Knowledge, Skills, and Abilities	Consistently assessed the knowledge, skills, and abilities of its workforce to tailor its awareness and specialized training and identified its skill gaps.
Training Comprehension Testing	Conducted multiple phishing exercises across the organization, ensured that all non-compliant users accounts were disabled, and ensured that an appropriate process is in place to obtain feedback on its security awareness and training program and uses that information to make improvements.

However, the Department's practices in all five of the metric questions still did not meet the Managed and Measurable level (***level 4***) of maturity or an effective level of security. The Department would need to achieve the Managed and Measurable level of security for at least three of the five metric questions to achieve an effective Security Training metric domain. For example, the Department would need to ensure that it addressed its identified knowledge, skills, and abilities gaps through training or talent acquisition.

Finding 6. The Department's Security Training Program Needs Improvement

We found that for the Security Training metric domain, the Department was at the Consistently Implemented for all five metric questions.

We did not identify new findings for the *Security Training* metric domain for FY 2021.

However, we found that corrective action plans for recommendations from previously reported findings were not implemented at the close of our audit fieldwork. This occurred because of the of Department's inconsistency in addressing and implementing prior audit recommendations. An ineffective security training program limits the Department's ability to ensure that its employees understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them.

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 2020 open recommendations include:

- **Recommendation 5.1.** To establish monitoring and oversight controls that ensure all new users satisfy all the mandatory training requirements before they receive access to Departmental resources.

This recommendation was reported in the FY 2020 FISMA audit report and is scheduled to be implemented by September 30, 2021,

Recommendations

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

SECURITY FUNCTION 3—DETECT

The Detect security function is comprised of the *ISCM* metric domain. Based on our evaluation of the Department's ISCM program, we determined the Detect security function was consistent with the Consistently Implemented level (***level 3***) of the maturity model, which is considered not 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 Consistently Implemented level (***level 3***) of the maturity model, which is considered not effective. However, we identified areas where the Department made improvements to its ISCM program. The Department remains at this level because of its inconsistency in addressing and implementing prior audit recommendations.

Progress Made in FY 2021

We found the Department took several actions to improve its information security continuous management posture as follows:

Areas Improved	Actions Taken
Policies, Procedures, and Standards	Defined and communicated its policies and procedures, established the ISCM Roadmap Timeline, ISCM Resource Management Plan, ISCM Continuous Diagnostics and Mitigation Onboarding Status Sheet Creation Standard Operating Procedure, ISCM Inventory Monitoring Standard Operating Procedure, FSA's ISCM Roadmap, and FSA's ISCM Guide.
Roles and Responsibilities	Roles and responsibilities are carried out as defined by policies and procedures at the enterprise level and at the system level; ISCM matters and other programs are discussed and communicated to stakeholders through the monthly Cybersecurity Risk Management workshop and Information System Security Officer meetings to discuss potential problems, new processes, and any emerging problems; and defined and documented the required system contacts in CSAM.
Enterprise-Wide ISCM Function	Published Cybersecurity Framework Risk Scorecard and CSAM Data Discrepancies Report in Microsoft Power BI, improved the Authorization to Operate process, and ensured system security plan processing.
Collecting and analyzing ISCM performance measures.	Consistently captured qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting.

However, the Department's practices in all four of its metric questions still did not meet the Managed and Measurable level (***level 4***) of maturity or an effective level of security. The Department would need to achieve the Managed and Measurable level of security for at least three of the four metric questions to achieve an effective Information Security Continuous Monitoring metric domain. For example, the Department would need to ensure that it integrates its metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization, explain the environment from both a threat or vulnerability and risk or impact perspective, and cover mission areas of operations and security domains.

Finding 7. The Department's Information Security Continuous Monitoring Program Needs Improvement

We found that for the ISCM metric domain, the Department was at the Consistently Implemented level for three metric questions and the Defined level for one metric question.

We did not identify new findings for the ISCM metric domain for FY 2021. However, we found that corrective action plans for recommendations from previously reported findings were not implemented at the close of our audit fieldwork. These conditions remain because the of the Department's inconsistency in addressing and implementing prior audit recommendations. An ineffective ISCM program limits the Department's

ability to monitor information systems to determine the ongoing effectiveness of deployed security controls, changes in information systems and environments of operation, and compliance with legislation, directives, policies, and standards.

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 2020 open recommendations include:

- **Recommendation 6.1**. To 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.

This recommendation was reported in the FY 2020 FISMA audit report and is scheduled to be implemented by September 30, 2021.

Recommendations

There are no new recommendations for the ISCM metric domain.

SECURITY FUNCTION 4—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 Consistently Implemented level (***level 3***) of the maturity model, which is considered not 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 to help the agency reach a higher level of maturity. For instance, we found that the data loss prevention tool is not working as intended.

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 determined that the Department's incident response program was consistent with the Consistently Implemented level (***level 3***) of the maturity model. Although some progress has been made, the Department remains at this level because the DLP tool was not fully operating as intended.

Progress Made in FY 2021

We found the Department took several actions to improve its incident response risk management posture as follows:

Areas Improved	Actions Taken
Policies, Procedures and Processes	Developed and updated a tailored incident response plan that highlights key components and capabilities; defined and communicated its policies, procedures, and processes for incident detection and analysis, incident handling, and reporting security incident information to the United States Computer Emergency Readiness Team, law enforcement, Congress (for major incidents) and OIG; implemented incident response policies, procedures, plans, and strategies, and consistently captured and shared lessons learned on the effectiveness of its incident response policies, procedures, plans, and strategies; monitors and analyzes qualitative and quantitative performance measures that have been defined in its incident response plan; and developed a new quality control process for reviewing the incidents on a weekly basis to assist the analysts and Education Security Operations Center managers in thoroughly completing tickets.
Roles and Responsibilities	Defined, communicated, and consistently implemented the structures of its incident response teams, roles and responsibilities of incident response stakeholders, and associated levels of authority and dependencies; designated a principal security operations center (Education Security Operations Center and FSA Security Operations Center) that is accountable to agency leadership, the Department of Homeland Security, and OMB for all incident response activities.
Incident Response Tools and Technologies	Utilized on-site, technical assistance or surge capabilities offered by the Department of Homeland Security and ensures that such capabilities can be leveraged when needed; utilized the Department of Homeland Security's Einstein 3 Accelerated to detect and proactively block cyber-attacks or prevent potential compromises; evaluated the effectiveness of its incident response technologies or tools and adjusts configurations and toolsets, as appropriate; consistently implemented its defined incident response technologies (in areas such as web application protections), event and incident management, and aggregation and analysis (such as security information and event management products); and worked directly with the Cybersecurity and Infrastructure Security Agency to analyze the 2020 SolarWinds cyberattack to determine how it affected the Department's network infrastructure and systems.

However, the Department's practices in five of the seven metric questions still did not meet the Managed and Measurable level (***level 4***) of maturity or an effective level of security. The Department would need to achieve the Managed and Measurable level of security for at least four of the seven metric questions to achieve an effective Incident Response metric domain. For example, the Department would need to ensure that it properly and adequately monitors and reviews the effectiveness of its data loss prevention (DLP) solution.

Finding 8. The Department's Incident Response Program Needs Improvement

We found that for the Incident Response metric domain, the Department was at the Managed and Measurable level for two metric questions, the Consistently Implemented level for three questions, and the Defined level for two metric questions. We determined that the Department's DLP tool was not functioning as intended and needs improvement. This occurred because the DLP tool was not properly configured and the Department did not adequately monitor the effectiveness of the tool. An ineffective incident response program could limit the Department's ability to rapidly detect incidents, minimize loss and destruction, mitigate any weaknesses to prevent future occurrences, and restore IT services.

Data Loss Prevention Tool Did Not Function as Intended

The Department's DLP SharePoint Online tool was operating effectively to prevent the transmission of Social Security numbers in accordance with Department policies. However, it was not properly configured to block and prevent the transmission of credit card numbers (CCN) outside of the Department's boundaries.

To comply with business standards and industry regulations, organizations must protect sensitive information, such as financial data, proprietary data, CCNs, health records, or Social Security numbers, and prevent its inadvertent disclosure. To help protect sensitive data and reduce risk, Agencies need a way to prevent users from inappropriately sharing sensitive data. The Department's DLP solution is driven by Federal requirements and regulated by the Department's standards for safeguarding PII and Sensitive PII, "Standard PR.DS: PII Data Loss Prevention—Microsoft Office 365."[15] These data protections are configured to operate with the Microsoft Office 365 application environment, specifically Microsoft Exchange email and SharePoint Online. The DLP solution identifies and flags known patterns for Social Security numbers and

[15] Sensitive PII includes but is not limited to Social Security Numbers, driver's license numbers, Alien Registration numbers, financial or medical records, biometrics, or a criminal history. This data requires stricter handling guidelines because of the increased risk to an individual if the data are compromised.

CCNs. For example, the policy requires that CCNs uploaded to a SharePoint portal in a 16-digit format: "XXXXXXXXXXXXXXXX" should be identified and blocked by the SharePoint Online Microsoft 365 DLP configuration.

The Department's SharePoint portal was established to help users share certain content with users that have a business need. This portal is used with internal and external users by providing a link to the data being shared from the Department's environment. We found that the DLP SharePoint online tool detected the distribution of Social Security numbers, according to the format specified within the Department policies. However, the tool failed to identify and detect the distribution of CCN data. OIG was able to successfully upload and distribute two file sets containing CCNs to an email address outside the Department's network without any warnings or being blocked. As a result, OIG evaded the Department's defenses and distributed a total of 53 CCNs to an external email address without being detected by the Department's DLP tool.

OIG activities were not captured or flagged by the Education Security Operations Center. The Departments' policy did not specify acceptable PII thresholds, and cited conflicting criteria, which creates inconsistent policy application. For example, in the criteria used to identify a CCN, the Department specified that there must be a text qualifier (i.e., "credit card") within 300 characters of the actual Social Security number, where it should state credit card number.

NIST SP 800-137, *ISCM for Federal Information Systems and Organizations*, states that an effective DLP strategy includes tools to monitor data at rest, in use, and in transit. In addition, as cited in NIST SP 800-53, the effective use of DLP technologies can assist organizations in automating the implementation, assessment, and continuous monitoring of several NIST SP 800-53 security controls.

The Department Standard PR.DS: PII Data Loss Prevention—Microsoft Office 365, details the minimum DLP requirements to prevent the intentional or accidental exposure of PII and Sensitive PII to unauthorized parties. Specifically, it establishes standards for CCNs, such as the Microsoft Office 365 DLP setting used by the Department to identify and prevent disclosure of CCNs. For example, the Microsoft SharePoint DLP configuration setting must identify CCNs and qualifier uploaded to SharePoint written in the 16-digit format: "XXXXXXXXXXXXXXXX". However, the Department did not properly or adequately monitor the effectiveness of its DLP solution. The DLP solution should be configured and applied consistently according to current policies to assure that users are not able to bypass the DLP defenses. It is imperative to improve the solution's capabilities to detect suspicious activity and validate its configuration to disallow the transmission of PII and Sensitive PII over SharePoint.

Without a properly configured DLP solution, in accordance with Departmental policy, a malicious user and insider threat actor could circumvent the DLP defenses and

potentially exfiltrate massive amounts of unencrypted CCN data without being detected or stopped. As a result, public confidence in the Department's abilities to protect personal financial information, such as CCNs, could decrease and cause serious damage to the Department's reputation.

Recommendation

We recommend that the Chief Information Officer require OCIO to—

8.1 Develop and implement improved monitoring procedures, and enhance current policies and processes, to ensure that the DLP solution works as intended for blocking of sensitive information transmission, as well as to ensure the detection of sensitive information with a higher degree of accuracy.

Department Comments

The Department agreed with Recommendation 8.1 and will develop a corrective action plan by December 31, 2021.

OIG Response

OIG will examine the proposed corrective action plan to determine whether the action will address the finding and recommendation and, if so, will validate this action during our FY 2022 FISMA audit.

SECURITY FUNCTION 5—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 Consistently Implemented level (***level 3***) of the maturity model, which is considered not effective. However, we noted some improvements were needed to help the agency reach a higher level of maturity.

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.

We determined that the Department's contingency planning program was consistent with the Consistently Implemented level (***level 3***) of the maturity model, although some improvements were made. The Department remains at this level because has not implemented oversight controls and addressed prior audit recommendations.

Progress Made in FY 2021

We found the Department took several actions to improve its contingency planning posture as follows:

Areas Improved	Actions Taken
Policies and Procedures	Defined its policies and procedures for providing contingency training consistent with roles and responsibilities.
Roles and Responsibilities	Roles and responsibilities of stakeholders have been defined and communicated across, including appropriate delegations of authority.
Business Impact Analysis and Contingency Plans and Testing	Consistently incorporated the results of organizational- and system-level Business Impact Analysis into strategy and plan development efforts, the information system security plans are consistently developed and implemented for systems, as appropriate, and include organizational and system-level considerations for activation and notification, recovery, and reconstitution; integrated system-level contingency plan development and maintenance activities with other continuity areas including organization and business process continuity, disaster recovery planning, incident management, insider threat implementation plan, and Occupant Emergency Plans; consistently implemented information system contingency plan testing and exercises; contingency plan testing and exercises are integrated, to the extent practicable, with testing of related plans, such as incident response plan, contingency of operations plan, or business continuity plan.
Backup and Storage	Defined its policies, procedures, processes, strategies, and technologies for information system backup and storage, including use of alternate storage and processing sites; considered alternative approaches when developing its backup and storage strategies including cost, environment, maximum downtimes, recovery priorities, and integration with other contingency plans; ensured that alternate processing and storage facilities are configured with information security safeguards equivalent to those of the primary site.
Communication of Planning and Performance	Effectively communicated recovery activities and communicated through the Cybersecurity Risk scorecard, as well as the Planning and Investment Review Working Group risk reporting process and the monthly Deputy Secretary briefing, also automated functionality of the Cybersecurity Risk scorecard.

However, the Department's practices in five of the six metric questions still did not meet the Managed and Measurable level of maturity or an effective level (***level 4***) of security. The Department would need to achieve a Managed and Measurable level of security for at least four of the six metric questions to achieve an effective Contingency Planning

metric domain. For example, the Department would need to ensure that their resources, people, processes, and technology are allocated in a risk-based manner for stakeholders to effectively implement system contingency planning activities.

Finding 9. The Department's Contingency Planning Program Needs Improvement

We found that for the Contingency Planning metric domain, the Department was at the Managed and Measurable level for one metric question, the Consistently Implemented level for three metric questions, and the Defined level for two metric questions.

We continue to find that the Department does not comply with contingency planning documentation requirements, including the lack of proper approval for its Business Impact Analysis. However, no new findings will be reported for the FY 2021 Contingency Planning metric domain since it is already captured within the open recommendations from the prior years (including FISMA FY 2020) to improve oversight controls over contingency planning documentation.

We found that corrective action plans for recommendations from previously reported findings were not implemented at the close of our audit fieldwork. The Department has not made significant efforts to address the conditions identified with contingency planning This occurred because of the of Department's inconsistency in addressing and implementing prior audit recommendations. An ineffective contingency planning program limits the Department's ability to recover information system services and data in an acceptable amount of time after a disruption.

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 2020 open recommendations include:

- **Recommendation 8.1**. To improve oversight controls that ensures contingency plan tests, and other artifacts impacting contingency plan testing, are documented, and updated in a consistent and timely manner.

- **Recommendation 8.2.** To develop additional processes and controls to confirm the proper validation and verification of all required contingency planning controls is documented accordingly before completing the SSP checklists and granting authorization to cloud service providers.

These recommendations were reported in the FY 2020 FISMA audit report and are scheduled to be implemented by September 30, 2021.

Recommendations

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

Appendix A. Scope and Methodology

Our objective was to determine whether the Department's overall IT security programs and practices were effective as they relate to Federal information security requirements. For FY 2021, the IG reporting metrics were organized around the five information security functions outlined in NIST's Framework for Improving Critical Infrastructure Cybersecurity: Identify, Protect, Detect, Respond, and Recover.

To answer the objective, we conducted audit work and additional testing in the nine metric domains associated with the security functions identified in the framework: (1) Risk Management, (2) Supply Chain Risk Management, (3) Configuration Management, (4) Identity and Access Management, (5) Data Protection and Privacy, (6) Security Training, (7) Information Security Continuous Monitoring, (8) Incident Response, and (9) Contingency Planning.

Specifically, we performed the following procedures:

- 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;
- assessed the Department's enterprise and system-level security controls;
- interviewed Department and FSA officials and contractor personnel, specifically staff with IT security roles, to gain an understanding of the system security and application management, operational, and technical controls;
- gathered and reviewed the necessary information to address the specific reporting metrics outlined in Department of Homeland Security's FY 2021 IG FISMA Metrics;
- obtained direct access to the Federal Risk and Authorization Management Program cloud service provider security packages for select systems; and
- compared and tested management, operational, and technical controls based on NIST standards and Department guidance.

In addition to conducting our own vulnerability scans, OIG contracted with an independent third-party contractor to perform additional vulnerability assessment and penetration testing scans on five FSA systems from May 2021 to July 2021. The contractor also conducted an adversarial simulation on one FSA system, tested controls on a government-furnished laptops and conducted a spear phishing exercise.

These results were incorporated in our overall assessment of the Department's cyber security posture. The specific results of our testing were provided to the Department and FSA for review and action.

We took additional testing steps to verify processes and procedures to:

- perform system-level testing for the Risk Management, Configuration Management, Data Protection and Privacy, and Contingency Planning metric domains;
- review corrective action plans identified starting from July 1, 2020, through July 2, 2021;
- test websites for encryption protocols and login banners;
- test and review the Department's virtual private network protocols and solution;
- identify users for compliance with the security training;
- review computer security incidents that were reported from July 1, 2020, to April 15, 2021;
- conduct a virtual walkthrough of the Department Security Operations Center and FSA Security Operations Center to examine their capabilities and resources on hand;
- perform vulnerability assessment testing on the five selected systems;[16]
- verify security settings for Department data protection;
- observe the 2021 Department's and FSA's disaster recovery tabletop exercises and test, which was conducted in a virtual setting;
- participate in the Department Cybersecurity Risk Management workshops; and
- conduct other security penetration testing as appropriate.

[16] Due to the COVID-19 pandemic and limited access to Department offices, we agreed to perform a limited security assessment testing for the FY 2021 FISMA audit to minimize the risk of Departmental system failure while the Department was operating at a 100 percent telework status. Therefore, we conducted limited web application testing, external network testing, database testing, and reviewed vulnerability scans provided directly by the Department.

We conducted our fieldwork from February 2021 through July 2021, primarily in a virtual setting due to the ongoing COVID-19 pandemic. We conducted an exit conference with Department and FSA officials on October 21, 2021.

Sampling Methodology

As of January 2021, the Department identified an inventory of 119 systems that were FISMA-reportable and classified as operational. Of the 119 FISMA-reportable systems, 88 were classified as moderate-impact systems, and 31 as low-impact systems.

During FISMA FY 2020, the OIG focused entirely on the testing Departmental systems part of the PIVOT environment. For the FISMA FY 2021, since most systems are managed by the FSA, and the prior two FISMA engagements concentrated on the PIVOT environment, OIG decided to focus exclusively on FSA systems, as well as on the progress in implementing OIG recommendations for the FISMA years 2018–2021, for both the Department and FSA. As a result, we selected a non-statistical sample of 5 out of 31 systems, which represented approximately 16 percent of all system in its relevant population and had a Federal Information Processing Standards Publication 199 impact level of either high or moderate.[17]

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, systems classified as cloud dependent, systems classified as not contractor owned, and systems containing PII.

Table 4 lists the judgmentally selected systems, the system's principal office, and the Federal Information Processing Standards Publication 199 potential impact level.

Table 4. Listing of Sampled Systems

Number	System Name	Principal Office	Impact Level
1	Access & Identity Management System	FSA	Moderate
2	Next Generation Data Center	FSA	Moderate
3	National Student Loan Data System	FSA	Moderate

[17] Federal Information Processing Standards Publication 199 defines three 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.

Number	System Name	Principal Office	Impact Level
4	Financial Management System	FSA	Moderate
5	Person Authentication Service	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.[18] In addition, all these systems were the focus of our system vulnerability assessment and testing.

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

- For Configuration Management, we tested all 633 Departmental websites for secure configurations for HTTP connection, encryption protocols, two-factor authentication, and login banners; inventory counts; and obsolete operating systems, applications, and databases.[19] Also reviewed 70 most recent, individual Nessus scan results supplied by the Department.
- For Data Protection and Privacy, we judgmentally sampled the Department's digital media sanitization processes for 10 out 479 employees and contractors subject to offboarding between October 1, 2020, and March 4, 2021.
- For Security Training, we tested a judgmental sample of 33 out of 166 new user accounts created from October 2020 to March 2021; we also tested a judgmental sample of 10 out of 584 employees and contractors that were required to complete role-based security training.[20]
- For Incident Response, we tested all 992 security events that occurred from July 1, 2020, through April 15, 2021, and examined 2 out of the 83 events that were deemed IT incidents.

[18] 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.

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

[20] The security training population was also used for testing within the Identity and Access Management.

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

Use of Computer-Processed Data

For this audit, 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 auditors did not have rights to access the system, or obtained directly by the auditors 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 audit. 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, the audit staff had direct access to the Department's and Federal Risk and Authorization Management Program's main security documentation repositories as a means of independent validations of the Department's provided data. As such, we determined this data was reliable for the purpose of our audit.

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

Appendix B. Comparison of Metric Maturity Level Scores (Fiscal Years 2020 and 2021)

Security Function	Metric Domain	FY 2020 Domain Maturity Level	FY 2021 Domain Maturity Level	FY 2020 Question Maturity Level	FY 2021 Question Maturity Level
Identify	Risk Management	Defined	Consistently Implemented	7 at Defined 4 at Consistently Implemented 1 at Optimized	3 at Defined **6 at Consistently Implemented** 1 at Optimized
Identify	Supply Chain Risk Management	N/A	Defined[21]	N/A	1 at Ad-Hoc 3 at Defined
Protect	Configuration Management	Consistently Implemented	Consistently Implemented	4 at Defined 2 at Consistently Implemented 2 at Managed and Measurable	3 at Defined **3 at Consistently Implemented** 2 at Managed and Measurable
Protect	Identity and Access Management	Defined	Defined	8 at Defined 1 at Managed and Measurable	7 at Defined 1 at Consistently Implemented
Protect	Data Protection and Privacy	Defined	Defined	4 at Defined 1 at Consistently Implemented	4 at Defined 1 at Consistently Implemented
Protect	Security Training	Defined	**Consistently Implemented**	3 at Defined 3 at Consistently Implemented	**5 at Consistently Implemented**

[21] Supply Chain Risk Management questions were part of the Risk Management metric questions on FISMA FY 2020 and prior. SCRM was not used to make an overall determination for the Identify function, but rather included for informational purposes only.

Security Function	Metric Domain	FY 2020 Domain Maturity Level	FY 2021 Domain Maturity Level	FY 2020 Question Maturity Level	FY 2021 Question Maturity Level
Detect	Information Security Continuous Monitoring	Defined	**Consistently Implemented**	3 at Defined 2 at Consistently Implemented	1 at Defined **3 at Consistently Implemented**
Respond	Incident Response	Consistently Implemented	Consistently Implemented	2 at Defined 4 at Consistently Implemented 1 at Managed and Measurable	2 at Defined 3 at Consistently Implemented **2 at Managed and Measurable**
Recover	Contingency Planning	Consistently Implemented	Consistently Implemented	1 at Defined 6 at Consistently Implemented	2 at Defined 3 at Consistently Implemented **1 at Managed and Measurable**

Appendix C. Status of Prior Year Recommendations

As part of this year's FISMA audit, we followed up on the status of prior year recommendations that were either closed during our fieldwork or continued to remain open after our fieldwork ended. If a recommendation remained open after our end of fieldwork date, we did not report on these findings and will follow-up in future FISMA audits to confirm if the corrective action is adequate. If recommendations were implemented and current year testing identified no findings, OIG closed the recommendations. If recommendations were partially implemented, not implemented at all, or we identified similar findings during our testing, we reopened the recommendations from prior years. Based on our testing we determined that

- for FY 2018, of the total of 45 recommendations made, 34 were reported as closed, and 11 remained open. Of the 34 closed recommendations, 4 were reopened because of our testing throughout FISMA FY 2021;
- for FY 2019, out of the total of 37 recommendations made, 27 were reported as closed, and 10 remained open. Of the 27 closed recommendations, 5 were reopened because of our testing this year; and
- for FY 2020, out of the total of 24 recommendations made, 4 were reported as closed while 20 remained open. Out of the four recommendations marked as closed, three were reopened based on the testing by the OIG.

The tables below show the open, closed, and reopened recommendations from FY 2018 through FY 2020.

FY 2018, OIG Audit Control Number A11S0001

Number	Recommendation	Status	PCD/ACD	OIG Determination
2.3	We recommend that the Deputy Secretary require OCIO to ensure that the configuration of 40 websites to be routed through a trusted internet connection or managed trusted internet protocol service.	Open	02/28/2022	Open

Number	Recommendation	Status	PCD/ACD	OIG Determination
2.2	We recommend 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. (Repeat Recommendation from FYs 2015, 2016, and 2017)	Closed	07/27/2020	Reopened
2.4	We recommend that the Deputy Secretary require OCIO to ensure that all existing websites and services are accessible through a secure connection as required by OMB M-15-13. (Repeat Recommendation from FY 2017)	Closed	07/27/2020	Reopened
3.3	We recommend that the Deputy Secretary and Chief Operating Officer require OCIO and FSA to enforce a two-factor authentication configuration for all user connections to systems and applications. (Repeat Recommendation from FYs 2011, 2012, 2013, 2014, 2015, 2016 and 2017)	Closed	07/28/2020	Reopened
3.4	We recommend that the Deputy Secretary require OCIO to finalize Departmental Directive OM: 5-101, "Personnel Security Screening Requirements for Contractor Employees."	Closed	07/06/2020	Closed

Number	Recommendation	Status	PCD/ACD	OIG Determination
3.5	We recommend that the Deputy Secretary require OCIO to fully implement the Department's ICAM strategy to ensure that the Department meets full Federal government implementation of ICAM. (Repeat Recommendation from FY 2017)	Closed	07/28/2020	Reopened
5.5	We recommend that the Deputy Secretary require OCIO to implement the process for identifying employees with significant security responsibilities and ensure role-based training is provided.	Closed	07/27/2020	Closed
6.3	We recommend that the Deputy Secretary require OCIO to ensure that ISCM stakeholders with designated roles and responsibilities are properly educated and engaged. (Repeat Recommendation from FY 2017)	Closed	07/13/2020	Closed
6.5	We recommend that the Deputy Secretary require OCIO to ensure the completion of Phases 1 and 2 of the Continuous Diagnostics and Mitigation program. (Repeat Recommendation from FY 2017)	Closed	01/28/2021	Closed

FY 2019, OIG Audit Control Number A11T0002

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.	Closed	07/27/2020	Reopened
2.5	We recommend that the Deputy Secretary require OCIO to ensure that all existing websites and services are accessible through a secure connection as required by OMB M-15-13.	Closed	07/27/2020	Reopened
2.6	We recommend that the Chief Operating Officer require FSA to discontinue the use of unsupported operating systems, databases, and applications.	Closed	09/09/2020	Reopened
3.5	We recommend that the Deputy Secretary require OCIO to fully implement the Department's ICAM strategy to ensure that the Department meets full Federal government implementation of ICAM. (Repeat Recommendation FYs 2018 and 2019)	Closed	07/27/2020	Reopened
3.9	We recommend that the Chief Operating Officer require FSA to enforce a two-factor authentication configuration for all user connections to systems and applications.	Closed	07/27/2020	Reopened
6.2	We recommend that the Deputy Secretary require OCIO to automate its capabilities for monitoring the security controls effectiveness and overall implementation of the ISCM Roadmap. (Repeat Recommendation FYs 2018 and 2019)	Open	10/29/2021	Open

Number	Recommendation	Status	PCD/ACD	OIG Determination
6.3	We recommend that the Deputy Secretary require OCIO to ensure the completion of Phases 1 and 2 of the Continuous Diagnostics and Mitigation program. (Repeat Recommendation FYs 2018 and 2019)	Open	01/28/2021	Closed
6.4	We recommend that the Deputy Secretary require OCIO to implement a process that ensures data reported on the Cybersecurity Framework Risk Scorecard is accurate.	Closed	10/08/2020	Closed

FY 2020, OIG Audit Control Number A11U0001

Number	Recommendation	Status	PCD/ACD	OIG Determination
2.5	We recommend that the Chief Information Officer require the Department to develop verification procedures and enforce the inactivity settings to ensure virtual private network sessions time out after 30 minutes of inactivity. (Incorporates a Repeat Recommendation)	Closed	02/16/2021	Reopened
3.2	We recommend that the Chief Information Officer require the Department to enforce the mandate for all websites to display warning banners when users login to Departmental resources and establish additional procedures and monitoring processes to ensure that banners include the approved warning language. (Incorporates a Repeat Recommendation)	Closed	07/12/2021	Reopened
7.3	We recommend that the Chief Information Officer require the Department to establish monitoring controls to ensure policies and procedures are updated frequently to contain the most updated information (i.e., contractual obligations) and those specifically relating to computer incident reporting to OIG are enforced accordingly.	Closed	02/16/2021	Closed

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)	Closed	03/02/2021	Reopened

Appendix D. CyberScope 2021 IG FISMA Metrics

Inspector General
Section Report

2021
IG Annual

Department of Education

For Official Use Only

Function 0: Overall

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

Not Effective

Comments: Not 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 determine whether the U.S. Department of Education's (Department) overall information technology (IT) security programs and practices were effective as they relate to Federal information security requirements. To answer this objective, we rated the Department's performance in accordance with FY 2021 Inspector General (IG) Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics. We determined the Department's programs were consistent with Level 2–Defined, which is considered not effective for three domains: Supply Chain Risk Management, Identity and Access Management, and Data Privacy and Protection, and Level 3–Consistently Implemented, which is considered not effective for six domains: Risk Management, 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. 4: CA-3, PM-5, and CM-8; NIST Cybersecurity Framework (CSF): ID.AM-1 - 4; FY 2021 CIO FISMA Metrics: 1.1, 1.1.5 and 1.4, OMB A-130, NIST SP 800-37, Rev. 2: Task P-18).

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 1. 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 the detailed information necessary for tracking and reporting (NIST SP 800-53 Rev. 4: CA-7 and CM-8; NIST SP 800-137; NIST IR 8011; Federal Enterprise Architecture (FEA) Framework, v2; FY 2021 CIO FISMA Metrics: 1.2, 1.3, 2.2, 3.9, CSF: ID.AM-1; NIST SP

Function 1A: Identify - Risk Management

800-37, Rev. 2: Task P-10).

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 1. 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 the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting (NIST SP 800-53 Rev. 4: CA-7, CM-8, and CM-10; NIST SP 800-137; NIST IR 8011; FEA Framework, v2; FY 2021 CIO FISMA Metrics: 1.2.5, 1.3.3, 1.3.9, 1.3.10, 3.10; CSF: ID.AM-2; NIST SP 800-37, Rev. 2: Task P-10)?

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 1. 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 2021 CIO FISMA Metrics: 1.1; OMB M-19-03; NIST SP 800-37, Rev. 2: Task C-2, C-3, P-4, P-12, P-13, S-1 - S-3, NIST IR 8170)?

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 1. The Department's Risk Management Program Needs Improvement

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. 4: RA-3, 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 P-2, P-3, P-14, R-2, and R-3?

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 1. The Department's Risk Management Program Needs Improvement

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 800-163, Rev. 1 CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 1. The Department's Risk

Function 1A: Identify - Risk Management

Management Program Needs Improvement

7. To what extent have the roles and responsibilities of internal and external stakeholders involved in cybersecurity risk management processes been defined, communicated, and implemented 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; NIST IR 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)?

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 1. The Department's Risk Management Program Needs Improvement

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-04-14, M-19-03, CSF v1.1, ID.RA-6)?

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 1. The Department's Risk Management Program Needs Improvement

9. To what extent does the organization ensure that information about cybersecurity risks is communicated in a timely and effective manner to appropriate internal and external stakeholders (OMB A-123; OMB Circular A-11 and OMB M-19-03; CSF: Section 3.3; NIST SP 800-37 (Rev. 2) Task M-5; SECURE Technology Act: s. 1326, NIST IR 8170 and 8286)?

Optimized (Level 5)

Comments: Optimized (Level 5)

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 and NIST IR 8286)?

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 1. The Department's Risk Management Program Needs Improvement

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/A21IT0023 (FISMA Report)

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

Function 1A: Identify - Risk Management

questions above and based on all testing performed, is the risk management program effective?

N/A

Function 1B: Identify - Supply Chain Risk Management

12. To what extent does the organization utilize an organization wide SCRM strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services? (The Federal Acquisition Supply Chain Security Act of 2018 (H.R. 7327, 41 USC Chap. 13 Sub chap. III and Chap. 47, P.L. 115-390) (Dec. 21, 2018), NIST SP 800-53, Rev. 5, PM-30, NIST IR 8276)?

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 2. The Department's Supply Chain Risk Management Program Needs Improvement

13. To what extent does the organization utilize SCRM policies and procedures to manage SCRM activities at all organizational tiers (The Federal Acquisition Supply Chain Security Act of 2018, NIST 800-53, Rev. 5, SR-1, NIST CSF v1.1, ID.SC-1 and ID.SC-5, NIST IR 8276)?

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 2. The Department's Supply Chain Risk Management Program Needs Improvement

14. To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization`s cybersecurity and supply chain requirements. (The Federal Acquisition Supply Chain Security Act of 2018, NIST SP 800-53 REV. 5: SA-4, SR-3, SR-5, 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).

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 2. The Department's Supply Chain Risk Management Program Needs Improvement

15. To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization`s systems? (800-53 rev 5 SR-11, 11 (1), and 11(2)

Ad Hoc (Level 1)

Comments: Ad Hoc (Level 1) - ED-OIG/A21IT0023 (FISMA Report), Finding 2. The Department's Supply Chain Risk Management Program Needs Improvement

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

Function 1B: Identify - Supply Chain Risk Management

Defined (Level 2)

Comments: Defined level (Level 2)

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

Consistently Implemented (Level 3)

Comments: Consistently Implemented level (Level 3) ED-OIG/A21IT0023 (FISMA Report)

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?

N/A

Function 2A: Protect - Configuration Management

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

Managed and Measurable (Level 4)

Comments: Managed and Measurable (Level 4) - ED-OIG/A21IT0023 (FISMA Report)

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)?

Managed and Measurable (Level 4)

Comments: Managed and Measurable (Level 4) - ED-OIG/A21IT0023 (FISMA Report)

19. To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53 REV. 4: CM-2 and CM-8; FY 2021 CIO FISMA Metrics: 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and PR.IP-1)?

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 3. The Department's Configuration Management Program Needs Improvement

20. To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53 REV. 4: CM-6, CM-7, RA-5, and SI-2; NIST SP 800-70, Rev. 4, FY 2021 CIO FISMA Metrics: 2.1, 2.2, 4.3; SANS/CIS

Function 2A: Protect - Configuration Management

Top 20 Security Controls 3.7; CSF: ID.RA-1 and DE.CM-8)?

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 3. The Department's Configuration Management Program Needs Improvement

21. To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53 REV. 4: CM-3, RA-5, SI-2, and SI-3; NIST SP 800-40, Rev. 3; SANS/CIS Top 20, Control 4.5; FY 2021 CIO FISMA Metrics: 1.3.7, 1.3.8, 2.13, 2.14; CSF: ID.RA-1; DHS Binding Operational Directives (BOD) 18-02 and 19-02)?

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 3. The Department's Configuration Management Program Needs Improvement

22. To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-19-26, DHS-CISA TIC 3.0 Core Guidance Documents)

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 3. The Department's Configuration Management Program Needs Improvement

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).

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 3. The Department's Configuration Management Program Needs Improvement

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)?

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 3. The Department's Configuration Management Program Needs Improvement

25.1. Please provide the assessed maturity level for the agency's Protect - Configuration Management program.

Consistently Implemented (Level 3)

Function 2A: Protect - Configuration Management

Comments: Consistently Implemented level (Level 3) - ED-OIG/A21IT0023 (FISMA Report)

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?

N/A

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 defined, communicated, and implemented 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 (FICAM) playbooks and guidance (see idmanagement.gov), OMB M-19-17)?

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 4. The Department's Identity and Access Management Program Needs Improvement

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; SANS/CIS Top 20: 14.1; DHS ED 19-01; CSF: PR.AC-4 and 5)?

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 4. The Department's Identity and Access Management Program Needs Improvement

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)?

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 4. The Department's Identity and Access Management Program Needs Improvement

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)?

Managed and Measurable (Level 4)

Comments: Managed and Measurable (Level 4) - ED-OIG/A21IT0023 (FISMA Report)

Function 2B: Protect - Identity and Access Management

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 non-privileged users to access the organization`s facilities [organization-defined entry/exit points], networks, and systems, including for remote access (HSPD-12; NIST SP 800-53 REV. 4: 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 2021 CIO FISMA Metrics: 2.4, 2.7, CSF: PR.AC-1 and 6; OMB M-19-17, and NIST SP 800-157)?

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 4. 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 (HSPD-12; NIST SP 800-53 REV. 4: AC-17, PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63 and 800-157; OMB M-19-17, FY 2021 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; and DHS ED 19-01)?

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 4. The Department's Identity and Access Management Program Needs Improvement

32. To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed (FY 2021 CIO FISMA Metrics: 2.3, 2.5, 2.6, and 2.7; OMB M-19-17, NIST SP 800-53 REV. 4: AC-1, AC-2, AC-5, AC-6, AC-17; AU-2, AU-3, AU-6, and IA-4; DHS ED 19-01; CSF: PR.AC-4).

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 4. 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 2021 CIO FISMA Metrics: 2.10 and 2.11).

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 4. The Department's Identity and Access Management Program Needs Improvement

Function 2B: Protect - Identity and Access Management

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

Defined (Level 2)

Comments: Defined level (Level 2) ED-OIG/A21IT0023 (FISMA Report)

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?

N/A

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), NIST Privacy Framework)?

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 5. The Department's Data Protection and Privacy Program Needs Improvement

36. To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle. (NIST SP 800-53 REV. 4; Appendix J, SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2021 CIO FISMA Metrics: 2.8, 2.12; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6)?
   - ·Encryption of data at rest
   - ·Encryption of data in transit
   - ·Limitation of transfer to removable media
   - ·Sanitization of digital media prior to disposal or reuse

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 5. The Department's Data Protection and Privacy Program Needs Improvement

37. To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (NIST SP 800-53 REV. 4: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2021 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5)?

Defined (Level 2)

Function 2C: Protect - Data Protection and Privacy

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 5. 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)?

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 5. The Department's Data Protection and Privacy Program Needs Improvement

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)?

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 5. The Department's Data Protection and Privacy Program Needs Improvement

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

Defined (Level 2)

Comments: Defined level (Level 2) ED-OIG/A21IT0023 (FISMA Report)

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?

N/A

Function 2D: Protect - Security Training

41. To what extent have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced? (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).

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 6. The Department's Security Training Program Needs Improvement

Function 2D: Protect - Security Training

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 (NIST SP 800-53 REV. 4: AT-2 and AT-3; 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/SANS Top 20: 17.1)?

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 6. The Department's Security Training Program Needs Improvement

43. To what extent does the organization utilize a security awareness and training strategy/plan that leverages its skills assessment and is adapted to its mission and risk environment? (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).

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 6. The Department's Security Training Program Needs Improvement

44. To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems? (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-1, AT-2; FY 2021 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-2; SANS Top 20: 17.4).

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 6. The Department's Security Training Program Needs Improvement

45. To what extent does the organization ensure that specialized security training is provided to individuals with significant security responsibilities (as defined in the organization's security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301) (NIST SP 800-53 REV. 4: AT-3 and AT-4; FY 2021 CIO FISMA Metrics: 2.15, and 5 Code of Federal Regulation 930.301)?

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 6. The Department's Security Training Program Needs Improvement

Function 2D: Protect - Security Training

46.1. Please provide the assessed maturity level for the agency's Protect - Security Training program.

Consistently Implemented (Level 3)

Comments: Consistently Implemented level (Level 3) ED-OIG/A21IT0023 (FISMA Report)

46.2. Please provide the assessed maturity level for the agency's Protect function.

Consistently Implemented (Level 3)

Comments: Consistency Implemented level (Level 3) ED-OIG/A21IT0023 (FISMA Report)

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?

N/A

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 800-37 (Rev. 2) Task P-7; NIST SP 800-137: Sections 3.1 and 3.6)?

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 7. The Department's Information Security Continuous Monitoring Program Needs Improvement

48. To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization (NIST SP 800-53 REV. 4: CA-1; NIST SP 800-137; CSF: DE.DP-1; NIST 800-37, Rev. 2 Task P-7 and S-5)

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 7. The Department's Information Security Continuous Monitoring Program Needs Improvement

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. 4: CA-2, CA-6, and CA-7; 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)

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 7. The Department's Information

Function 3: Detect - ISCM

Security Continuous Monitoring Program Needs Improvement

50. How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 7. The Department's Information Security Continuous Monitoring Program Needs Improvement

51.1. Please provide the assessed maturity level for the agency's Detect - ISCM domain/function.

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report)

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?

N/A

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)?

Managed and Measurable (Level 4)

Comments: Managed and Measurable (Level 4) - ED-OIG/A21IT0023 (FISMA Report)

53. To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization (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 2021 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 8. The Department's Incident Response Program Needs Improvement

54. How mature are the organization's processes for incident detection and analysis? (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; OMB M-20-04; CSF: DE.AE-1, DE.AE-2 -5, PR.DS-6, RS.AN-1 and 4, and PR.DS-8; and US-CERT Incident Response Guidelines)

Function 4: Respond - Incident Response

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 8. The Department's Incident Response Program Needs Improvement

55. How mature are the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2)

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 8. The Department's Incident Response Program Needs Improvement

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)

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 8. The Department's Incident Response Program Needs Improvement

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).

Managed and Measurable (Level 4)

Comments: Managed and Measurable (Level 4) - ED-OIG/A21IT0023 (FISMA Report)

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)

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 8. The Department's Incident Response Program Needs Improvement

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

Function 4: Respond - Incident Response

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report)

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?

N/A

Function 5: Recover - Contingency Planning

60. To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined, communicated, and implemented across the organization, including appropriate delegations of authority (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)?

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 9. The Department's Contingency Planning Program Needs Improvement

61. To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34, Rev. 1, 3.2; NIST IR 8286; FIPS 199; FCD-1; OMB M-19-03; FY 2021 CIO FISMA Metrics, Section 5; CSF:ID.RA-4)?

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 9. The Department's Contingency Planning Program Needs Improvement

62. To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34; FY 2021 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 9. The Department's Contingency Planning Program Needs Improvement

63. To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST SP 800-34; NIST SP 800-53 REV. 4: CP-3 and CP-4; FY 2021 CIO FISMA Metrics, Section 5; CSF: ID.SC-5 and CSF: PR.IP-10)?

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report), Finding 9. The Department's Contingency

Function 5: Recover - Contingency Planning

Planning Program Needs Improvement

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 2021 CIO FISMA Metrics, Section 5; and NARA guidance on information systems security records)?

Defined (Level 2)

Comments: Defined (Level 2) - ED-OIG/A21IT0023 (FISMA Report), Finding 9. The Department's Contingency Planning Program Needs Improvement

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)?

Managed and Measurable (Level 4)

Comments: Managed and Measurable (Level 4) - ED-OIG/A21IT0023 (FISMA Report)

66.1. Please provide the assessed maturity level for the agency's Recover - Contingency Planning domain/function.

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report)

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?

N/A

APPENDIX A: Maturity Model Scoring

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

Function 1A: Identify - Risk Management

Function	Count
Ad-Hoc	0
Defined	3
Consistently Implemented	6
Managed and Measurable	0
Optimized	1
Calculated Rating: Consistently Implemented (Level 3)	
Assessed Rating: Consistently Implemented (Level 3)	

Function 1B: Identify - Supply Chain Risk Management

Function	Count
Ad-Hoc	1
Defined	3
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Calculated Rating: Defined (Level 2)	
Assessed Rating: Defined (Level 2)	

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	0

APPENDIX A: Maturity Model Scoring

Defined	3
Consistently Implemented	3
Managed and Measurable	2
Optimized	0
Calculated Rating: Consistently Implemented (Level 3)	
Assessed Rating: Consistently Implemented (Level 3)	

Function 2B: Protect - Identity and Access Management

Function	Count
Ad-Hoc	0
Defined	7
Consistently Implemented	0
Managed and Measurable	1
Optimized	0
Calculated Rating: Defined (Level 2)	
Assessed Rating: Defined (Level 2)	

Function 2C: Protect - Data Protection and Privacy

Function	Count
Ad-Hoc	0
Defined	4
Consistently Implemented	1
Managed and Measurable	0
Optimized	0
Calculated Rating: Defined (Level 2)	

APPENDIX A: Maturity Model Scoring

Assessed Rating: Defined (Level 2)

Function 2D: Protect - Security Training

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	5
Managed and Measurable	0
Optimized	0

Calculated Rating: Consistently Implemented (Level 3)

Assessed Rating: Consistently Implemented (Level 3)

Function 3: Detect - ISCM

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	3
Managed and Measurable	0
Optimized	0

Calculated Rating: Consistently Implemented (Level 3)

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	2

APPENDIX A: Maturity Model Scoring

Consistently Implemented	3
Managed and Measurable	2
Optimized	0
Calculated Rating: Consistently Implemented (Level 3)	

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	0
Defined	2
Consistently Implemented	3
Managed and Measurable	1
Optimized	0
Calculated Rating: Consistently Implemented (Level 3)	

Overall

Function	Calculated Maturity Level	Accessed Maturity Level	Explanation
Function 1: Identify - Risk Management / Supply Chain Risk Management	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented level (Level 3) ED-OIG/A21IT0023 (FISMA Report)
Function 2: Protect - Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistency Implemented level (Level 3) ED-OIG/A21IT0023 (FISMA Report)
Function 3: Detect - ISCM	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report)
Function 4: Respond - Incident Response	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report)

APPENDIX A: Maturity Model Scoring

Function 5: Recover - Contingency Planning	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3) - ED-OIG/A21IT0023 (FISMA Report)
Overall	**Not Effective**	**Not Effective**	**Not Effective**

Appendix E. Acronyms and Abbreviations

CCN	Credit Card Number
CSAM	Cyber Security Assessment and Management
Department	U.S. Department of Education
DLP	Data Loss Prevention
FISMA	Federal Information Security Modernization Act of 2014
FSA	Federal Student Aid
FY	Fiscal Year
HSTS	Hypertext Transfer Protocol Secure Strict Transport Security
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
ICAM	Identity, Credential, and Access Management
IG	Inspector General
ISCM	Information Security Continuous Monitoring
IT	Information Technology
NIST	National Institute of Standards and Technology
O365	Microsoft Office 365
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIVOT	Portfolio of Integrated Value-Oriented Technologies
POA&M	Plan of Action and Milestones

SAOP	Senior Agency Official for Privacy
SCRM	Supply Chain Risk Management
SORN	System of Records Notice
SP	Special Publication
SSL	Secure Socket Layer
TLS	Transport Layer Security

Department Comments

UNITED STATES DEPARTMENT OF EDUCATION

DATE: October 26, 2021

TO: Robert D. Mancuso
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 2021
Control Number ED-OIG/A21IT0023

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) 2021 Draft Report, Control Number ED-OIG/A21IT0023. The Department recognizes that 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. The Department is committed, and has taken numerous steps, to strengthen the overall cybersecurity of its networks, systems, and data, as reflected in the draft report.

During FY 2021, the Office of the Chief Information Officer (OCIO) successfully continued to support IT services to support 100% telework in response to the COVID-19 pandemic. Despite the continued 100% telework, there was no significant impact or compromise to the Department Information Security Program, and it allowed the Department to continue its important mission without interruption. Additionally, the Department did not have any major information security incidents occur, despite the challenging work environment necessitated by the COVD-19 pandemic. In addition, the Department has developed a close working relationship with the FedRAMP Project Management Office (PMO) which allowed us to establish more reoccurring continuous monitoring meetings with participating agencies to help improve the security posture of those Cloud Service Providers.

During FY 2021, the Department has been recognized for its diligence and performance in responding to Department of Homeland Security (DHS) Emergency Directives, including the mitigation of the SolarWinds Orion Code Compromise and the Microsoft Exchange On-Premises Product Vulnerabilities. The Department performed considerably well in comparison to other agencies based on publicly available data regarding incident responses.

The Department participated in an Assessment Evaluation and Standardization High Value Asset (AES-HVA) Beta three-day course that taught participating members how to apply the DHS AES-HVA assessment methodology at their organizations. As a result of this effort, DHS invited the Department, in partnership with FSA, to present at the April 14, 2021, CISO Council HVA Sub-Committee Meeting. The

400 MARYLAND AVE. S.W., WASHINGTON, DC 20202
www.ed.gov

request came from CISA's HVA Project Manager, to highlight the success of this engagement and the Department's outstanding partnership with the HVA Program.

The Department was recently acknowledged for its early and successful adoption of the Department of Homeland Security's Federal High Value Asset Enterprise Prioritization methodology. Utilizing this methodology, the Department collected and reviewed IT system information in order to calculate and prioritize risk values for all Department FISMA-reportable systems. These risk values were used to determine systems that met the threshold of a high value asset. As a result of this effort, the Department identified four additional IT systems that have been added to the Department's HVA Program.

The Department's Cybersecurity Training Program Manager (PM) was nominated and awarded the FY 2021 Federal Information Systems Security Educator's Association (FISSEA) Cybersecurity Awareness and Training Innovator Award in recognition of innovation, dedication, and impact in moving our Department's cybersecurity training program forward. Each year at the annual conference, FISSEA recognizes an individual who has made significant contributions in inspiring the strategic planning, building, and management of innovative cybersecurity awareness and training programs. Nominees may be involved in any aspect of cybersecurity awareness and training, including, but not limited to; cyber instructional curriculum developers, cybersecurity instructors, cybersecurity program managers, workforce development managers, and practitioners who further awareness and training activities or programs.

In FY 2021, The Department was invited to participate in a Proof of Value (PoV) pilot effort with CISA to build clear and concise instructions on how to implement a Cyber Supply Chain Risk Management (C-SCRM) program that is sustainable in varying organizational environments. The Department has been recognized by CISA for contributing thought leadership in establishing parameters for an effective ICT SCRM program in collaboration with several Federal agencies and non-profit organizations.

The Department was acknowledged for its comprehensive and thorough submission and the mission justification for funding allocation, via the Technology Modernization Fund (TMF), to support modernization in creating and implementing a zero-trust architecture (ZTA) plan.

In FY 2021, the Department was invited to participate and present its CSF Risk scorecard to OMB. The OMB attendees noted the Department's CSF Risk Scorecard implementation in Power BI was the among the most effective tools they had seen to convey cybersecurity risks in a comprehensive and actionable capacity.

In FY 2021, the Department was approached to provide a demonstration of its cybersecurity risk scoring and visualization capabilities to the Department of Commerce (DOC). As a result of the Department's demonstration of risk scoring and visualization capabilities, DOC has expressed considerable interest in establishing similar capabilities within their cybersecurity mission space.

During FY 2021 the Department collaborated with General Services Administration (GSA) and several cabinet-level Federal agencies to develop and establish organizationally defined control parameter values for NIST SP 800-53, Revision 5 control implementation. The Department was recognized for considerable contributions to this collaboration by GSA's working group participants. Outcomes of this effort directly contributed to Department policy enhancements.

The Department appreciates the work of the OIG on this audit and believes two of the identified recommendations are either already being addressed by work efforts identified in prior audit cycles or being managed through the Department's existing risk management processes. The remaining

recommendations will be addressed through corrective action plans developed by OCIO.

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 3.1: Take steps to assure obsolete solutions and encryption protocols are either updated, removed, or replaced.

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2022 and will develop a corrective action plan by December 31, 2021 to address the recommendation.

OIG Recommendation 3.2: Implement additional measures for patches to be applied in a timely manner based on a priority basis.

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2022 and will develop a corrective action plan by December 31, 2021 to address the recommendation.

OIG Recommendation 3.3: Ensure all Department websites are configured to mask PII when used as an identifier.

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2022 and will develop a corrective action plan by December 31, 2021 to address the recommendation.

OIG Recommendation 3.4: Enforce secure connections as required by OMB M-15-13 for all existing websites and services.

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2022 and will develop a corrective action plan by December 31, 2021 to address the recommendation.

OIG Recommendation 3.5: Require FSA to take immediate corrective actions to mitigate the vulnerabilities identified during the vulnerability assessment.

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2022 and will develop a corrective action plan by December 31, 2021 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 4.1: Fully implement ICAM Strategy by established milestones to ensure the Department meets full Federal government implementation of ICAM.

Management Response: The Department concurs with this recommendation. The Department was able to implement the ED ICAM solution but was not able to leverage it to its full potential during the FY21 audit period. The Department will continue implement the ICAM Strategy in FY 2022 and will develop a corrective action plan by December 31, 2021, to address this recommendation.

OIG Recommendation 4.2: Take steps to ensure user activity is terminated on the FSA Next Generation Data Center after 30 minutes.

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2022 and will develop a corrective action plan by December 31, 2021 to address the recommendation.

OIG Recommendation 4.3: Document 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 2022 and will develop a corrective action plan by December 31, 2021 to address the recommendation.

OIG Recommendation 4.4: Enforce a two-factor authentication configuration for all user connections to systems and applications.

Management Response: The Department partially concurs with this recommendation. The Department must have the ability to have exemptions and not all systems/users are required to have MFA based on the type of information the systems share or the type of data that is used/stored by the system. The Department will continue to ensure that all relevant system meet this requirement in FY 2022 and will develop a corrective action plan by December 31, 2021, for any valid systems that are found to not be in compliance with the two-factor authentication configuration requirements.

OIG Recommendation 4.5: Perform and evidence regularly scheduled reviews of system user accounts (both privileged and non-privileged) to recertify and maintain each Department system's validity.

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2022 and will develop a corrective action plan by December 31, 2021 to address the recommendation.

OIG Recommendation 4.6: Remove terminated users' access to Department resources timely in accordance with Departmental policy.

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2022 and will develop a corrective action plan by December 31, 2021 to address the recommendation.

OIG Recommendation 4.7: Identify and enforce all websites to display warning banners when users login to Departmental resources.

Management Response: The Department partially concurs with this recommendation. The Department must have the ability to have exemptions and not all websites are required to have warning banners. The Department will continue to ensure that all applicable websites have warning banners in FY 2022 and will develop a corrective action plan by December 31, 2021, for any applicable websites that currently do not have warning banners.

OIG Recommendation 4.8: Take immediate corrective actions to mitigate the vulnerabilities identified during the endpoint vulnerability assessment.

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2022 and will develop a corrective action plan by December 31, 2021 to address the recommendation.

OIG Recommendation 4.9: Establish and enforce a corrective action plan to monitor and remediate identified database vulnerabilities.

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2022 and will develop a corrective action plan by December 31, 2021 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 5.1: 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.

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2022 and will develop a corrective action plan by December 31, 2021 to address the recommendation.

REPORTING METRIC DOMAIN No.8: INCIDENT RESPONSE

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

Recommendation 8.1: Develop and implement improved monitoring procedures, and enhance current policies and processes, to ensure that the DLP solution works as intended for blocking of sensitive information transmission, as well as to ensure the detection of sensitive information with a higher degree of accuracy.

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2022 and will develop a corrective action plan by December 31, 2021 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:

Steven Hernandez, Director, Information Assurance Services, Office of the Chief Information Officer
Dan Commons, Director, Information Technology Risk Management Group, 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