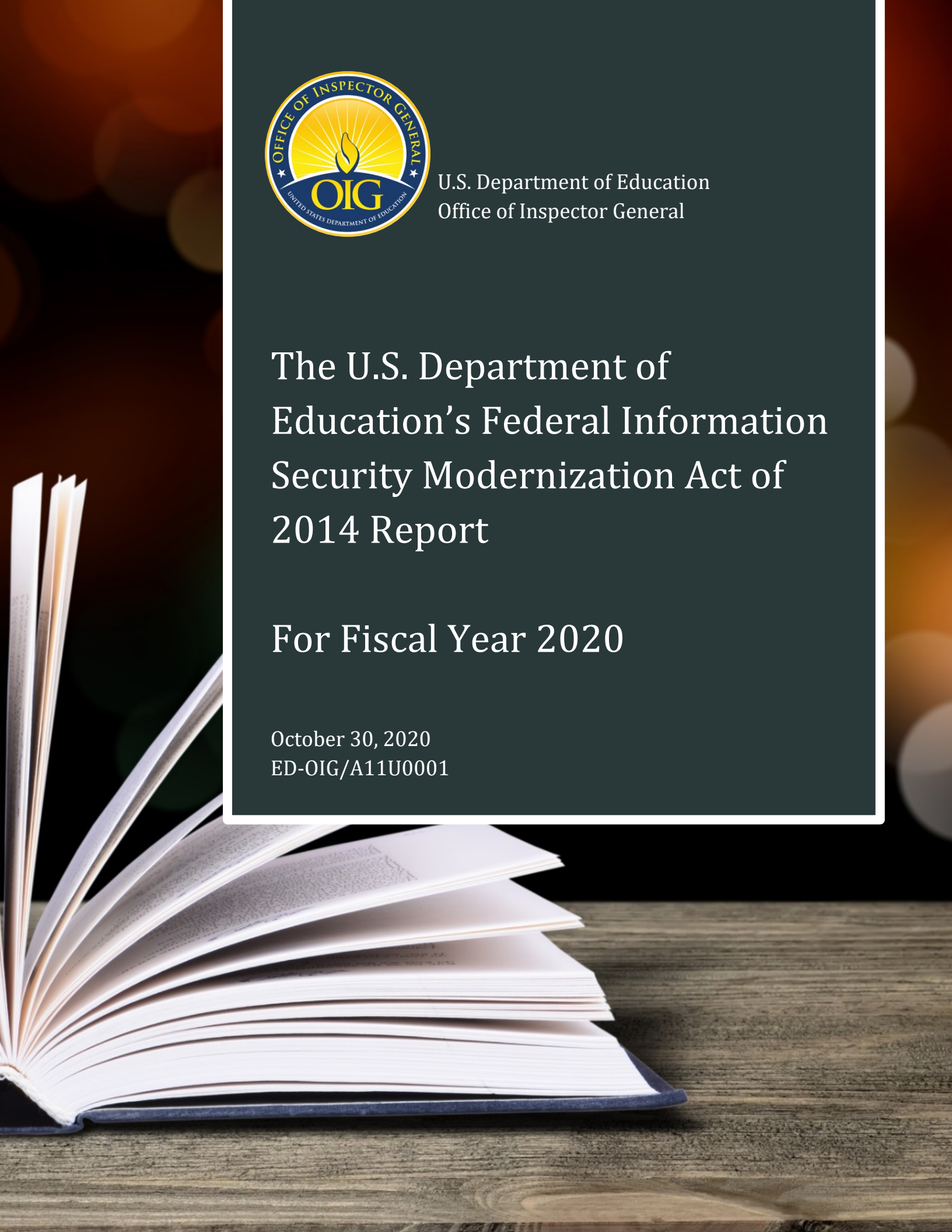


U.S. Department of Education
Office of Inspector General

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

For Fiscal Year 2020

October 30, 2020
ED-OIG/A11U0001

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.

UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Information Technology Audit Division

October 30, 2020

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 2020
Control Number ED-OIG/A11U0001

Attached is the subject final audit report that covers 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 2020. 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:

Mitchell Zais, PhD, Deputy Secretary, Office of the Secretary and Deputy Secretary
Diane Auer Jones, Principal Deputy Under Secretary, Delegated the Duties of the Under Secretary, Office of the Under Secretary
Ann Kim, Deputy Chief Information Officer, Office of the Chief Information Officer
Mia Jordan, Chief Information Officer, Federal Student Aid

Wanda Broadus, Deputy Chief Information Officer, Federal Student Aid
Steven Hernandez, Chief Information Security Officer, Office of the Chief Information Officer
Dan Commons, Director, Enterprise Cybersecurity Group, Federal Student Aid
James Wolfe, Audit Liaison, Office of the Chief Information Officer
Stefanie Clay, Audit Liaison, Federal Student Aid
Phil Rosenfelt, Deputy General Counsel, Office of the General Counsel
L'Wanda Rosemond, Audit Accountability and Resolution Tracking System Administrator, Office of Inspector General

Table of Contents

Results in Brief

What We Did

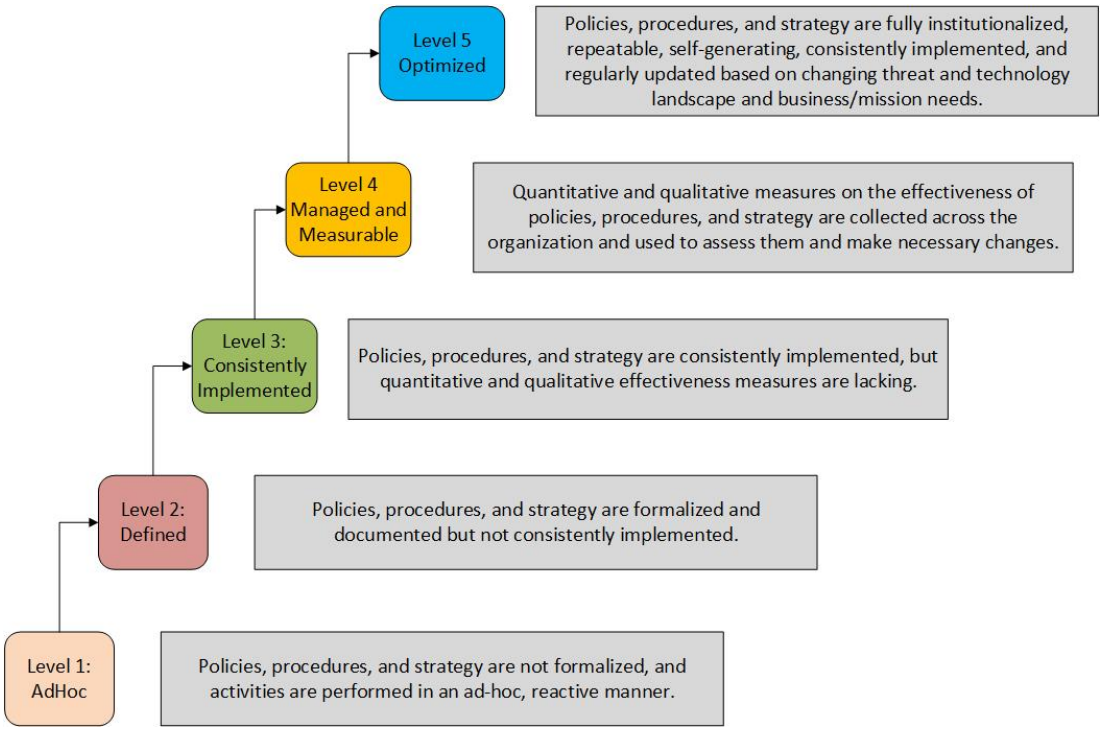
Our objective was to determine whether the U.S. Department of Education's (Department) overall information technology (IT) security programs and practices were effective as they relate to Federal information security requirements. To answer this objective, we rated the Departments performance in accordance with Fiscal Year (FY) 2020 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 eight metric domains (as outlined in the National Institute of Standards and Technology's "Framework for Improving Critical Infrastructure Cybersecurity").

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
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

In accordance with the FY 2020 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. Maturity Level and Description



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

Although the Department had several notable improvements in implementing its cybersecurity initiatives, its overall IT security programs and practices were not effective in all of the five security functions. We had findings in all eight metric domains, which included findings with the same or similar conditions identified in prior reports. To further assist the Department, we included items that did not reach the level of a finding within the Other Matters section of this report.

We determined the Department's programs were consistent with

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

None of the Department domains were rated **Level 1, Ad-Hoc**, which has the greatest risks. Also, the *Configuration Management* and *Incident Response* metric areas have both improved from **Level 2, Defined** (cited during our FY 2019 audit), to **Level 3, Consistently Implemented**.

For FY 2020, the Department has improved on several individual metric scoring questions, especially in the areas of *Risk Management*, *Incident Response* and *Contingency Planning*. The Department also demonstrated improvement in its processes from FY 2019 within several metric areas. Appendix B shows the three domain improvements along with all the Department's metric maturity level ratings by domain and by the number of questions for FYs 2019 and 2020.

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

- *Risk Management.* Remediation process for its Plan of Action and Milestones; enterprise supply chain assessment strategy; IT inventory reporting; and required IT security clauses for its contracts.

- *Configuration Management*. Use of unsecure connections and appropriate application connection protocols; and reliance on unsupported operating systems, databases, and applications in its production environments.

- *Identify and Access Management*. Removing access of terminated users to the Department's network and database management.

- *Incident Response*. Timely reporting of incidents; and ensuring data loss prevention tools work accordingly.

Until the Department improves in these areas, it cannot ensure that its overall information security program adequately protects its systems and resources from compromise and loss.

In addition, we reported on the status of the Department's Cybersecurity Policy Framework implementation and a system authorization issue that we discovered towards the end of our audit fieldwork. This issue is discussed in the Other Matters section of this report. Finally, we followed up on the status of prior year findings and the implementation of corrective actions from the last three FISMA audits (FY 2017–FY 2019) 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 2020 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 31, 2020.

What We Recommend

We made 24 recommendations (8 of which are repeat recommendations) in all 8 metric domains to assist the Department with increasing the effectiveness of its information security programs. 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 2 shows the number of recommendations we made by security function and metric domain, including the sum of repeat recommendations from prior years' audits.

Table 2. Recommendations Made by Security Function and Domain

Security Function	Domain	Recommendations	Repeat
Identify	Risk Management	5	2
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training	11	5
Detect	Information Security Continuous Monitoring	1	-
Respond	Incident Response	4	1
Recover	Contingency Planning	3	-

In response to a draft of this report, the Department concurred with 5 recommendations, partially concurred with 16 recommendations, and did not concur with 3 recommendations. We summarized and responded to the Department's response at the end of each finding and included the full text of the Department's comments at the end of this report (see Department Comments). We considered the Department's comments and as a result of subsequent evidence provided, we revised Finding 5 but did not make any revisions to recommendation 5.1. The Department was not required to and did not provide any additional information regarding the Other Matters section of this 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) 2020 Inspector General FISMA Metrics V 4.0 (FY 2020 IG FISMA Metrics), issued on April 17, 2020. Our audit focused on reviewing the five security functions and eight associated metric domains for cybersecurity management.

Background

FISMA Requirements and Responsibilities

The E-Government Act of 2002 (Public Law 107-347) recognized the importance of information security to the economic and national security interests of the United States.[1] Title III of the E-Government Act of 2002, which was amended in 2014, commonly referred to as FISMA,[2] 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 (1) reestablishing the oversight authority of the Director of OMB with respect to agency information security policies and practices and (2) setting forth

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

[2] 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.

authority for the Department of Homeland Security Secretary to administer the implementation of such policies and practices for information systems. FISMA also provides several modifications that modernize Federal security practices to address evolving security concerns. These changes result in less overall reporting, stronger use of continuous 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 2020 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 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 (1) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems and (2) an assessment of the effectiveness of the information security policies, procedures, and practices of the agency.

FY 2020 Inspector General FISMA Reporting Metrics

The Council of the Inspectors General on Integrity and Efficiency, OMB, and Department of Homeland Security developed the FY 2020 IG FISMA Metrics, in consultation with the Federal Chief Information Officer Council. The FY 2020 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 2020 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 eight 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. In accordance with FISMA and OMB Memorandum M-20-04, "Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements," all Federal agencies are to submit their IG metric results and determinations into the Department of Homeland Security's CyberScope application by October 31, 2020, included in Appendix D.

Department's Information Technology Investments

The Department's FY 2020 total spending for information technology (IT) investments was estimated at $844 million, which included $481 million in spending on major IT investments (57 percent of total spending). This is a 26.2 percent increase from the FY 2017 total spending of $669 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. This approach is very different from the previous model, the Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) contract, which combined all service areas into one primary contract.[3]

[3] The EDUCATE contract officially ended on July 31, 2019.

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 their operational parameters set in their contracts.
- PIVOT-P – managed print services for the Department.

The contracts were awarded between 2017 and 2018, with transition activities occurring between 2018 and 2019. The Department completely transitioned its IT infrastructure services to the PIVOT environment on July 31, 2019. As of June 9, 2020, the Department deployed 5,370 workstations, 872 multi-function devices, and 78 new scanning devices with proven new technologies to improve its ability become more modern, faster, and cost-effective.

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 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.

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

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

In addition to OCIO, Federal Student Aid (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 2019 FISMA audit, we identified 8 findings and provided 37 recommendations in all 8 metric domain areas that addressed the conditions noted in the report, with a majority of the recommendations made in the Protect and Detect security functions. The Department concurred with 31 recommendations, partially concurred with 4, and did not concur with 2. As of July 2020, the Department and FSA reported that they had completed corrective actions for 16 of the 37 recommendations. The Department and FSA are scheduled to complete all the remaining corrective actions by end of FY 2021, except for one that has been extended to February 2022.

See Appendix C for complete details regarding prior year FISMA audit recommendations, and the status of corrective actions for FYs 2017, 2018, and 2019.

Audit Results and Findings

We had findings in all eight 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 2017 through 2019.

SECURITY FUNCTION 1—IDENTIFY

The Identify security function comprises the *Risk Management* metric domain. Based on our evaluation, we determined that the Identify security function was consistent with Level 2: Defined, which is considered not effective. While the Department continues to develop and strengthen its risk management program, we noted that improvements were needed in the Department's supply chain strategy, corrective action plan remediation process, IT reporting, and the inclusion of IT security clauses for contracts.

METRIC DOMAIN 1—RISK MANAGEMENT

We determined that the Department's risk management program was consistent with the Defined level of the maturity model, which is considered not effective although some improvements have been made. Risk management embodies the program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, and reputation), organizational assets, staff, and other organizations. This includes establishing the context for risk-related activities, assessing risk, responding to determined risk, and monitoring risk over time. It also includes agencies developing a corrective action plan to assist them in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

Progress Made in FY 2020

We found the Department took several actions to improve its risk management posture regarding policies and procedures, roles and responsibilities and communications to stakeholders, inventory management, Cyber Security Assessment and Management (CSAM) and System Security, and Enterprise-wide solutions.

Policies and Procedures
• established policies and procedures consistent with NIST standards; defined, communicated, and implemented policies and procedures for conducting system level risk assessments; and developed a series of new standards designed to strengthen its risk management program ("Standard ID.GV: Required Authorization Documentation," issued February 12, 2020), for developing, managing, and maintaining a system security plan (SSP), including narratives, appendices, and artifacts which support the SSP and also, ("Standard ID.GV: SSP Review," issued February 11, 2020), related to requirements for SSPs prior to signature.
Roles, Responsibilities, and Communications
• defined and communicated across the organization roles and responsibilities of risk management stakeholders; and conducted workshops and forums to inform stakeholders on risk management issues.
Inventory Management
• defined a process to develop and maintain a comprehensive and accurate inventory of its information systems and system interconnections using the CSAM system; defined importance and priority levels for its information systems considering risks from the supporting business functions and mission impacts, including for high value assets.
CSAM and System Security
• implemented a process to ensure Plan of Action and Milestones (POA&Ms) are approved and input into the system of record, CSAM; achieved a 94 percent net reduction in open POA&Ms since October 1, 2019; continued to incorporate the Risk Management Framework into CSAM to provide system owners and other shareholders with the capabilities of addressing the requirements of the Risk Management Framework (including categorization and monitoring); and continued the practice of disseminating CSAM discrepancy reports to its information systems security officers and information system owners to facilitate updates to selected CSAM records for systems displaying poor data quality.
Enterprise-Wide Solutions
• consistently implemented a security architecture across the enterprise, business process, and system levels; identified and defined its requirements for an automated solution that provides a centralized, enterprise wide view of risks across the Department; continued its use of an enterprise-wide Cybersecurity Framework Risk Scorecard, published monthly, to communicate the Department's risks to all its stakeholders. The Cybersecurity Framework Risk Scorecard was enhanced with an increased detection of data integrity issues and incorporation of privacy scoring.

However, the Department's practices in 11 of the 12 metric questions still did not meet the Managed and Measurable level of maturity or an effective level of security. The Department would need to achieve a Managed and Measurable level of security for at least 7 of the 12 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. Based on our review, we noted improvements were needed in the Department's (1) corrective action plan remediations , (2) enterprise supply chain assessment strategy process, (3) IT inventory reporting and (4) incorporating IT security clauses in contracts. Finding 1 identifies the areas needing improvement for this metric domain in greater detail.

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

We found that for the *Risk Management* metric domain, the Department was at the Optimized level for one metric question, the Consistently Implemented level for four metric questions, and the Defined level for seven metric questions. The Department concurred with our 2019 recommendation to incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Risk Management program, and agreed to complete this task by September 30, 2021; therefore, we did not reissue this recommendation for this year.

We determined that the Department's controls for the corrective action plan process needed improvement, enterprise supply chain assessment strategy was not fully defined and implemented, there was inconsistency in IT inventory reporting, and inconsistency in enforcing and monitoring required IT security clause inclusions for its contracts. This occurred because the Department's remediation and inventory processes were primarily manual efforts, and the supply chain management policies and procedures were not fully defined or implemented. As a result, this metric domain is considered not effective. An ineffective risk management program limits the Department's ability to establish a well working process for managing information security risks.

The Department's Corrective Action Plan Remediation Process Needs Improvement

The Department did not provide effective oversight of its corrective action plan remediation process. The corrective action plan process is part of the Department's Cyber Risk Management Framework Strategy. The Cyber Risk Management Framework focuses on an active continuous monitoring approach that incorporates maintaining awareness of the security state of information systems on an ongoing basis through enhanced monitoring. The Department utilizes CSAM as the system of record for monitoring and the remediation of POA&Ms. CSAM is also the primary data feed for the Cyber Security Framework (CSF) scorecard dashboard.

We found that 106 of 1,211 POA&Ms created from October 2017 to March 2020 were not remediated within the required timeframe. In addition, 72 POA&Ms were not

assigned a criticality impact level that provides security professionals a means of prioritizing POA&M reduction and remediation efforts. The format is standard for all Departmental POA&Ms. At a minimum, this requires that specific data elements must be defined for each security vulnerability entered in CSAM. The User Defined Criticality impact level as defined by the assessment source (Low, Medium, High) is a required data element for all POA&M's.

NIST Special Publication (SP) 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," requires agencies to update existing corrective action plans on the organization-defined frequency based on the finding from security controls assessments, security impact analyses, and continuous monitoring activities. It further requires organizations to employ automated mechanisms to help ensure that the POA&Ms for the information system is accurate, up-to-date, and readily available. The corrective action plan process is also part of the Department's Cybersecurity Risk Management Framework Strategy's Monitor Risk Factors, where it is required to coordinate with information system security officers to work corrective action plan items and completion dates in the authorization decision process.

Furthermore, according to the Departments POA&M Standard Operating Procedure, Version 1.8, dated February 20, 2020, the following fields are required for each identified POA&M entered into CSAM: System Name, Discovered, Source, Title, Description, Recommendation, Milestone 1 (Mitigation Strategy), Scheduled Completion Date, Associated Security Controls, User Defined Criticality, Threat Description, Assigned, and Notes. Additionally, scheduled completion dates for corrective action plans are based on user-defined criticality levels.

The Department continues to rely on manual and ad-hoc processes to update, manage, and monitor POA&Ms entered into CSAM rather than an automated mechanism to help ensure that the POA&Ms for the information system are accurate, up to date, and readily available. The Department continues to be aware of the data inaccuracy and integrity issues in CSAM and utilizes the CSF scorecard discrepancy reporting tool to identify selected data inaccuracies. Untimely remediation of POA&Ms, along with incomplete and inaccurate information, inhibits the Department's abilities to assess risk and funding requirements, properly analyze weaknesses, determine whether actions have been taken, and implement Department-wide solutions. We reported a similar condition in the FY 2018 and 2019 FISMA audits.

Supply Chain Strategy Not Fully Defined and Implemented

The Department has not fully defined and implemented an Enterprise Supply Chain Assessment Strategy that includes supply chain risk tolerance, acceptable supply chain risk mitigation strategies, and foundational practices. This includes (1) defined oversight roles and responsibilities for the Information and Communications Technology (ICT)

supply chain; (2) a methodology that includes foundational practices[5] and (3) a process for evaluating and monitoring supply chain risk associated with the development, acquisition, maintenance, and disposal of systems.

The Department has initiated some foundational practices, but they have not been fully defined and/or implemented. Specifically, we found the Department has incorporated an ICT performance component into the CSF Scorecard, but has not fully implemented the supply chain risk to reflect the Department's current environment. The CSF scorecard is used to define risk profiles and align and prioritize its cybersecurity activities within its business and mission requirements, risk tolerance and appetite, and resources. Currently, the Department's CSF Scorecard reflects a risk score of 3 out of 3 for OCIO indicating no supply chain risk to OCIO systems.

In accordance with NIST SP 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," supply chain risk management is an organization-wide activity that should be directed under the overall agency governance, regardless of the specific organizational structure. Additionally, NIST SP 800-161 requires having foundational practices in place, which is critical to successfully and productively interacting with mature system integrators and suppliers who may have such practices standardized and in place. Furthermore, in accordance with Circular A-130, revised in 2016, agencies shall consider information security, privacy, records management, public transparency, and supply chain security issues for all resource planning and management activities throughout the system development life cycle so that risks are appropriately managed.

The Department indicated it is working toward efforts to communicate and implement risk management policies, procedures, and strategy to include an action plan for supply chain management. The Department informed us they planned to start this process in August 2020. The Department also stated it is working with the Department of Energy toward an action plan for supply chain risk management. Because the Department did not adequately define nor consistently implement current policies and procedures, it did not have enough information to fully define its supply chain strategy. Without a defined supply chain strategy that includes oversight roles and responsibilities, the Department's ICT supply chain risks may go undetected and unnoticed. These ICT supply

[5] Foundation practices include (1) a process to conduct supply chain risk management review of potential supplier prior to awarding a contract or issuing an order to a supplier for ICT products and services; (2) procedures to perform assessments of ICT supply chain risk; (3) developing ICT supply chain risk management requirements for suppliers; and (3) procedures for detecting counterfeit and compromised ICT products to their deployment.

chain risks include, but are not limited to, insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the ICT supply chain.

Inconsistency in IT Inventory Reporting

The Department uses CSAM as its primary system of record for tracking, managing, and reporting on Cyber Risk Management Framework implementation and as a component of Cyber Risk Management Framework governance. All additions and dispositions of systems to the inventory are required to be approved by the Enterprise Architecture Review Board. In addition, all shared services (cloud service providers) are also required to be registered in the Department's IT inventory within CSAM and categorized appropriately and accordingly.

We found that the Department was unable to provide sufficient information to validate the completeness of current IT inventory. Specifically, we requested evidence to determine if the Department verifies whether Department system, cloud service provider, website, and mobile device inventories are comprehensive and accurate. Based on our analysis, we found problems with these inventories:

- System Assets. The Department was unable to provide sufficient evidence to validate the completeness of current system asset inventory. For example, the PIVOT asset inventory provided did not contain complete system details, such as the system version. We also identified 652 blank entries.
- Cloud Service Providers. The Department maintains a comprehensive and accurate inventory of cloud systems. However, these shared services are not accurately recorded within the primary system of tracking, CSAM. Currently, the Department records and tracks the Departments cloud service providers in the Department's Shared Services Portfolio SharePoint site outside of CSAM.
- Websites. We were provided a current inventory of all websites currently managed by the Department and FSA. We independently developed our own inventory of Departmental websites and based on our analysis, found that nine websites were not included in the FY 2020 inventory provided by the Department.
- Mobile Devices. The Department utilizes a mobile device management solution for its mobile devices for managing access to the Department's enterprise services. The Department could not provide adequate information to demonstrate the accuracy of its mobile device inventory, such as mobile phones on hand that have not been activated or disposed of properly.

NIST SP 800-53, Revision 4, CM-8 – Information System Component Inventory, states that organizations should develop and document an inventory of information system

components that (1) accurately reflects the current information system, (2) includes all components within the authorization boundary of the information system, and (3) is at the level of granularity deemed necessary for tracking and reporting. It further states that the organization should update the inventory of information system components as an integral part of component installations, removals, and information system updates and provide a centralized repository for the inventory of information system components.

In addition, IAS-02: OCIO/IAS Policy Framework Instruction – Identify, dated February 3, 2020, states that Information System Owners and Information System Security Officers, in coordination with the Chief Information Security Officer, must develop, maintain, regularly review, and update within CSAM an inventory of all Department information system hardware and software, to include those assets of systems operated on behalf of the Department. The inventory must accurately reflect the information system; include all components within the authorization boundary of the system; and be conducted at the level of granularity necessary for the purposes of inventory tracking and reporting.

Lastly, in accordance with Departmental memorandum "Department of Education's Plan of Action to Implement 21st Century Integrated Digital Experience Act," issued in March 2020, each principal office is required to review its current inventory of websites, digital services and non-digital services to produce a baseline inventory and report on its current compliance with the 21st Century Integrated Digital Experience Act.

The Department relies on manual and ad-hoc procedures to verify the accuracy of its inventory. Therefore, the Department does not have the assurance that CSAM contains the most accurate and complete information to manage its systems and device inventory. Failure to identify a complete and accurate inventory, specifically one that accurately reflects all assets, shared service providers, and active websites managed by the Department, increases the risk a system or device will not be identified or misidentified, and could lead to compromise and exposure of data without the Department knowing that it had occurred.

Contracts Did Not Include Security Control Compliance and Access Language

The Department did not have a consistent process to enforce and monitor inclusion of required IT security clauses for its contracts. We judgmentally selected six contracts and contract modifications that were signed after October 1, 2019, and reviewed them for required IT security clauses. We found that all six were not consistent in including required IT security clauses.

The Department's "Standard ID.SC: Security and Privacy Language for IT Procurements," dated February 2020, requires cybersecurity language to be incorporated into all IT contracts. The Department informed us that it developed a standard agency-wide process for performing reviews of IT contracts and technical standards related to cybersecurity, personal security, and privacy to implement Department-wide standardized contract language. However, the Department has not consistently implemented this requirement as identified by the condition noted above. Unless all required standard privacy, security, and access clauses and provisions are included in its service contracts, the Department cannot ensure that contractors and service providers fully understand the information security and privacy regulations, mandates, and requirements to which they will be subject to under the contract or task order. This puts the Department's systems and data at further risk of a loss of confidentiality, integrity, and availability. We reported similar conditions in our FY 2017 and 2018 FISMA audits.

Recommendations

We recommend that the Chief Information Officer require the Department to—

1.1 Establish oversight controls to ensure that POA&Ms are assigned with the required criticality impact levels and remediation is conducted within the required timeframes. (Incorporates a Repeat Recommendation)

1.2 Develop and implement a Department-wide ICT supply chain risk management strategy to include the supply chain risk tolerance, acceptable supply chain risk mitigation strategies, and foundational practices.

1.3 Develop a process to evaluate and routinely monitor supply chain risks associated with the development, acquisition, maintenance, and disposal of systems and products.

1.4 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.[6] (Incorporates a Repeat Recommendation)

1.5 Verify and periodically reconcile the accuracy of cloud service provider inventories in or against CSAM.

[6] Both Recommendations 1.1 and 1.4 incorporate repeat recommendations that the Department previously closed. Our review identified that the findings remained; therefore, we decided to reopen the recommendations so the Department can take further action to correct the problems identified.

Department Comments

The Department partially concurred with Recommendations 1.1, 1.2, 1.3, 1.4, and 1.5. For Recommendation 1.1, it stated that it views criticality as being consistently and appropriately applied per the latest POA&M standard operating procedure leveraging "control risk severity," assigns a control risk severity based upon the National NIST control associated with each POA&M, and utilizes its Most Valuable Progress report to prioritize POA&M reduction and remediation efforts. It agreed remediation within established timeframes can be improved, and it will develop a corrective action plan by December 31, 2020 to address the recommendation.

For Recommendation 1.2, the Department stated that nearly all of its supply chain risk management information communication technology concerns relate to services, and based on the requirements from statutory law, executive orders and NIST, a Department-wide supply chain risk management information communication technology program was neither required nor cost effective until the "B" provision (August 2020) of the 2019 National Defense Authorization Act was required. The Department has re-assessed, and subsequently, re-categorized the two previous "High" impact systems to "Moderate" impact and performed necessary actions to meet the requirements of section 889 of the Act. The Department is currently developing a Department-wide supply chain risk management information communication technology program in alignment with the Department's established risk tolerance. The Department agreed that opportunities exist to establish further supply chain risk reduction strategies in accordance with the Federal Acquisition Security Council and will develop a corrective action plan by December 31, 2020 to address the recommendation.

For Recommendation 1.3, the Department stated that its acquisition processes include specific acquisition alerts requiring vendors to make representations regarding their adherence to supply chain risk management, it developed procedures and instructions to ensure compliance with the requested actions, and it issued Acquisition Alerts to address evolving threats specific to supply chain. OCIO also awarded a new contract in the fourth quarter of FY 2020 to further enhance the supply chain risk management information communication technology program. The Department agrees further processes and procedures will be required as the Federal Acquisition Security Council, OMB, and NIST provide further instructions and guidance. The Department will develop a corrective action plan by December 31, 2020, to address this recommendation.

For Recommendation 1.4, the Department explained that per the NIST Information System Component Inventory control CM-8 enhancement (2), the associated automation requirements apply to "High" impact systems, which do not apply to Department systems, as there are currently no "High" impact systems in its inventory. Hardware and software lists are required at the system level and monitored for completeness through the required authorization documentation risk factor in the daily

CSF Risk Scorecard and Security Documentation Status Report. The Department agreed that there are opportunities to improve the reconciliation of inventories between systems and external sources such as FedRAMP. The Department will continue this effort in FY 2021 and will develop a corrective action plan by December 31, 2020, to address this recommendation.

Regarding the security requirements in contracts, the Department disagreed. It stated that five of the six contracts reviewed by the OIG include provision 3452.239-72, which is enforceable language that addresses cybersecurity requirements outlined in Department "Standard ID.SC: Security and Privacy Languages for IT Contracts." The Department stated that one of the five contracts had the clause included in the blanket purchase agreement and that clauses flow down from the blanket purchase agreement to the respective task orders, and that the sixth contract was a simplified purchase of IT licenses with no services provided. Therefore, the requirements are not applicable.

For Recommendation 1.5, the Department explained its leveraged cloud service providers are registered in CSAM and it provides the full list of Department authorized cloud service providers in other locations and formats. The Department enhanced its daily CSAM Data Discrepancies report in the fourth quarter of FY 2020 to monitor the cloud service provider data field in CSAM to ensure accurate capture and will continue to enhance quality assurance procedures to manage the cloud service provider inventory more effectively across all applicable sources. The Department agrees it has an opportunity to further enhance this process to ensure immutable evidence of reconciliation can be provided and will develop a corrective action plan by December 31, 2020, to address this recommendation.

OIG Response

OIG will review the corrective action plans to determine whether the actions will address the finding and recommendations and, if so, will validate them during our FY 2021 FISMA audit.

Regarding Recommendation 1.1, we noted in our report that the Department made significant progress in this area. However, as stated in the finding, according to Departmental standards, user-defined criticality is a required element that must be defined for each POA&M entered into CSAM. In addition, the Department did not address the identified issue, but rather identified manual processes in place that are not commensurate with a preventative control. Therefore, we found opportunities for improvement.

For Recommendation 1.2 and 1.3, OIG acknowledges the Department's position surrounding the supply chain risk management information communication technology requirements; however, our position remains unchanged. OIG understands the two

systems the Department references were later reassessed to moderate impact; however, the fact is that during our audit scope period and the beginning stages of our audit, the Department's system inventory included two systems that were categorized as high impact systems. OIG will review and validate the described actions the Department is taking to address its supply chain risk management program, during our FY 2021 FISMA audit.

For Recommendation 1.4, OIG will continue to monitor the Department's progress in implementing this recommendation. As stated above, while there are currently no high impact systems in the Department's inventory, there were high impact systems during our audit scope and the beginning of our audit. Automating or establishing preventative controls should still be part of the corrective action plan, particularly as the Department could have high impact systems in the future. Regarding the contract issue, the Department's response conflicts with its own standards. According to "Standard ID.SC: Security and Privacy Languages for IT Contracts," all contracts must contain the specific required language referenced for acquisitions and license agreements. OIG will monitor the Department's proposed corrective action plan and review this issue in further detail during our FY 2021 FISMA audit.

For Recommendation 1.5, OIG acknowledged the evidence provided by the Department during the audit. However, OIG auditors attempted and were not able to extract an accurate list of cloud service providers from CSAM, nor the CSF Scorecard. When we requested additional information from the Department we were directed to a SharePoint site and told to rely on a spreadsheet containing the most accurate cloud service provider data, as this was the source of cloud service provider information for the CSF scorecard, and not CSAM.

SECURITY FUNCTION 2—PROTECT

The “Protect” security function comprises 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 Defined level of the maturity model, which is considered not effective.

METRIC DOMAIN 2—CONFIGURATION MANAGEMENT

We determined that the Department’s configuration management program was consistent with the Consistently Implemented level of the maturity model, which is considered not effective. 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.

Progress Made in FY 2020

We found that the Department took several actions to improve its configuration management program regarding policies and procedures, roles and responsibilities and communications to stakeholders, baseline configurations, change control board, trusted internet connection solutions, and network access control.

Policies and Procedures
• developed, documented, and disseminated an enterprise wide configuration management plan and comprehensive policies and procedures for managing the configurations of its information systems, and common secure configuration (hardening guides) that are tailored to its environment including deviation processes; created a standard for remediation information system vulnerabilities identified by Department of Homeland Security Cyber Hygiene scanning; and established an Information Technology Security Baseline Configuration Guidance that provides a uniform approach for installation, configuration, and maintenance of secure information technology system baseline configurations.
Roles and Responsibilities
• held stakeholders involved in information system configuration management accountable for carrying out their roles and responsibilities effectively.
Baseline Configurations
• consistently recorded, implemented, and maintained baseline configurations of its information systems and an inventory of related components in accordance with the organization's policies and procedures; used its “Baseline Cybersecurity Standard OCIO-STND-01” to ensure compliance with basic applicable system configuration requirements and assisted principal offices with the necessary security concepts to manage and maintain security baseline configurations; and followed the OMB-mandated Federal Desktop Core Configuration.
Change Control
• established a change control board referred to as Enterprise Architecture Review Board; and deployed its endpoint management platform called “BigFix,” which protects workstations and servers by achieving a high rate first-pass patch success rate and enabling continuous endpoint compliance across Windows, UNIX, Linux, and Macintosh operating systems.

Trusted Internet Connections and Network Access Control Solutions
• implemented trusted internet connection solutions by ensuring all end-user Internet traffic from the Department's networks or via virtual private network connections or traffic from Department managed networks and hosting environments is routed through a trusted internet connection; and implemented the network access control solution at its Potomac Center Plaza location, which blocks all non-government furnished equipment devices from connecting to the network and will quarantine non-compliant government furnished equipment to a remediation virtual local area network for patching and compliance updating.

However, the Department's practices in six of the eight areas still did not meet the Managed and Measurable level 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 needs to ensure that all obsolete systems are retired and replaced by a new solution. Finding 2 identifies the areas needing improvement for this metric domain in greater detail.

Finding 2. The Department's Configuration Management Programs Need 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 two metric questions, and the Defined level for four metric questions. We determined the Department's controls needed improvement for using appropriate application connection protocols; relying on vendor-supported operating systems, databases, and applications in its production environment; ensuring virtual private network connections disconnect after 30 minutes of inactivity; consistently performing system patching; and improving controls over web applications and servers. This occurred because the Department continues to rely on weak encryption protocols for its connections, depend on incomplete remediation processes, and inconsistently enforcing its defined processes and configurations—especially those within its virtual private network settings and web applications. As a result, this metric domain is considered not effective. 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 Continue to Run Outdated Protocols on Authorized Websites

We found that the Department and FSA have not fully disabled and discontinued use of outdated secure connection protocols. Our testing validated that websites continue to

use weak, vulnerable, and obsolete protocols to encrypt traffic in transit. Specifically, we identified that 5 out of the 572 tested sites continue to use Transport Layer Security (TLS) 1.0 to encrypt traffic, and 41 of the tested sites are also configured to use TLS 1.1. OIG also conducted a vulnerability assessment testing during which time Nessus scans identified several deficiencies, including the continued use of Secure Sockets Layer, TLS 1.0, and TLS 1.1 protocols to encrypt traffic in transit. While the Department has made significant progress since last year in its decrease in the use of TLS 1.1, which was reported as 197 sites last year, it still needs to strengthen its 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 2017, 2018, and 2019 FISMA audits.

NIST SP 800-52, "Guidelines for the Selection, Configuration and Use of Transport Layer Security Implementations," states that TLS version 1.1 is required, at a minimum, to mitigate various attacks on version 1.0 of the TLS protocol. Servers that support 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.[7] However, the Department and FSA have not disabled the option to use weak encryption protocols, such as Secure Sockets Layer, TLS 1.0, and TLS 1.1. The Department lacked proper controls that would have ensured these weak encryption protocols be 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 Are Not Being Applied in a Timely Manner

We found that the Department did not consistently apply software patches and security updates to its systems and IT solutions timely. Most notably, we identified systems that were missing critical patches, making them vulnerable to attacks. We also identified systems that had not migrated to newer and supported versions of security solutions (older versions being obsolete). The Department did not consistently implement and lacked proper controls for enforcing its vulnerability and patch management policies and standards. Failure to patch systems in a timely manner could expose Department systems and solutions to a malicious exploit, leakage of data, damage, or unintended

[7] NIST SP 800-52, Revision 2, "Guidelines for TLS Implementations", states Protocol Version Support Servers that support 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.

exposure of sensitive information. It is imperative to assure that patches are applied in a timely manner to those identified as exploitable vulnerabilities, for which patches are disseminated. We reported similar conditions in our FY 2017, 2018, and 2019 FISMA audits.

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

We found that the Department and FSA still relied on several systems and applications that were not supported by the vendors. In reviewing the Department's configuration management database, we found that for 1,341 systems and applications listed, 72 were identified as running with obsolete operating systems. In addition, obsolete solutions, such as unsupported operating systems and outdated software, were identified during our system security assessment testing. The Department and FSA officials confirmed that a process has been established to track obsolete applications and systems for remediation. However, the Department lacked proper controls to enforce the management of unsupported system components, specifically unsupported operating systems, databases, and applications. Continued use of obsolete systems will make these IT solutions vulnerable to intentional and unintentional compromise. Further, relying on unsupported operating systems, databases, and applications, could lead to data leakage and exposure of personally identifiable information (PII) that can compromise the Department's integrity and reputation. Systems that reach their "end of life" cycle are no longer supported and patched by the vendor and can become vulnerable to new exploits such as post-retirement "zero-day" and other malicious attacks.[8] We reported similar conditions in our FY 2017, 2018 and 2019 FISMA audits.

Virtual Private Network Connection Did Not Time Out After 30 Minutes of Inactivity

During our testing of the Department's new virtual private network connection solution, we determined that the solution was not configured to disconnect a user after 30 minutes of inactivity. Department officials informed us that the vendor made the proper configuration setting to ensure users were disconnected after 30 minutes of inactivity. However, our testing validated that the connection remained online for over one hour without being disconnected. Therefore, the Department did not ensure the correct configuration setting was applied. Without properly testing the virtual private network time-out feature functionality, there is an increased risk that users could expose the

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

Department's networks to unauthorized users and compromise the confidentiality, integrity, and availability of information systems.

Department's Controls over Web Applications and Servers Need Improvement

The Department's web-applications vulnerabilities increase the risk of unauthorized access to critical security architecture. We assessed web application security for two of the eight systems judgmentally selected for testing. For both systems, we found that the Department had not appropriately implemented and managed its technical security architecture supporting OCIO web applications and infrastructure to restrict unauthorized access to information resources and protect against application compromise. Specifically, we identified instances of (1) reflected cross-site scripting, (2) website cookie vulnerabilities, (3) cross-domain misconfiguration, (4) the need for better content security policy enhancement, (5) missing patches, and (6) moderately weak cipher suites and protocols. We determined 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 (1) baseline configuration, (2) unsupported system components, and (3) transmission confidentiality and integrity.[9]

Additionally, NIST SP 800-63 Revision 3, "Digital Identities Guidelines," states that reauthentication of a user shall be repeated following any period of inactivity lasting 30 minutes or longer and that the session shall be terminated (i.e., logged out).

[9] Includes control numbers CM-2, DM-1, SA-22, SC-8, and IA-5.

Recommendations

We recommend that the Chief Information Officer require the Department to—

2.1 Incorporate additional measures to, at a minimum, achieve Level 4 Managed and Measurable status of the Configuration Management program.

2.2 Develop enhanced oversight controls to ensure all Department connections are migrated to TLS 1.2 or higher cryptographic protocol. (Incorporates a Repeat Recommendation)

2.3 Enhance implementation controls to prioritize and apply the most up-to-date and timely software patches and security updates to the identified systems and information technology solutions.

2.4 Establish stronger monitoring controls to enforce the management of unsupported system components and track and discontinue the use of unsupported operating systems, databases, and applications. (Incorporates a Repeat Recommendation)

2.5 Develop verification procedures and enforce the inactivity settings to ensure virtual private network sessions time out after 30 minutes of inactivity.[10] (Incorporates a Repeat Recommendation)

2.6 Correct or mitigate the vulnerabilities identified during the security assessment, in accordance with the severity level of each vulnerability identified.

Department Comments

The Department concurred with Recommendation 2.1 and will develop a corrective action plan by December 31, 2020. For Recommendation 2.6, the Department concurred and stated that several of the vulnerabilities found were already covered under preexisting Risk Acceptances Forms and/or POA&Ms. The Department will continue to monitor those POA&Ms and Risk Acceptance Forms in accordance with Department policies and acknowledges that there are opportunities to improve. For any remaining identified vulnerabilities, the Department will develop a corrective action plan by December 31, 2020.

The Department partially concurred with Recommendations 2.2, 2.3, and 2.4. For Recommendation 2.2, the Department stated that it conducts periodic scans of external

[10] Recommendations 2.2, 2.4 and 2.5 incorporate repeat recommendations that the Department previously closed. However, our review identified that the findings remained; therefore, we reopened the recommendations so the Department can take further action to correct the problems identified.

web sites and validation of information systems and services to check for compliance to TLS version 1.2. In the event that a site is identified as out of compliance, immediate outreach occurs and the issue is either resolved or a POA&M is created to monitor the resolution of the vulnerability in accordance with the Department's POA&M standard operating procedure. In addition, the Department's TLS and Forward Secrecy working group meets regularly to review and prioritize remediation of impacted systems. The Department agreed that it needs to continue ensuring that all of its connections are migrated to TLS 1.2 or higher, and will continue managing TLS risk in FY 2021. Upon verification and validation of OIG's test data, it will develop a corrective action plan by December 31, 2020.

For Recommendation 2.3, the Department stated that in FY 2020, it enhanced its vulnerability management program to support the proper evaluation of vulnerability management and the unification of vulnerability management technology and programs across the Department's IT infrastructure. As part of oversight management controls, if identified vulnerabilities are unable to be remediated within the timeframe established in Department guidance, a POA&M is developed, monitored, and remediated through the Department's POA&M management process. The Department agreed that vulnerability management controls should be enhanced on an ongoing basis in the balance of the mission, technology, and feasibility. The Department will develop a corrective action plan by December 31, 2020.

For Recommendation 2.4, the Department stated that as a part of its IT modernization and migration to new providers, the software requirements in the contracts only allow for N-1 proposed solutions, which means hardware or services can only be one version behind the current version. Additionally, the Department can extend support for end of life or service system components by up to six months or longer depending on the vendor. Any identified unsupported system components are monitored and remediated through the Department's POA&M management process. The Department requested OIG's test results for verification and validation, and upon receipt, the Department will develop a corrective action plan by December 31, 2020.

The Department did not concur with Recommendation 2.5. It explained that OMB rescinded Memorandum M-07-16 that mandated the use of a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes of inactivity. While OMB M-17-25 requires the timeout of remote connections after 30 minutes of inactivity, neither memo specifies if user or system activity is the criteria for which the 30 minutes timeout applies. The Department also, referenced NIST SP 800-53, Revision 4, which addresses the termination of user-initiated logical sessions and the termination of network connections. It does not mandate specific timeframes or the use of user inactivity, but rather permits the use of organization-defined conditions or trigger events requiring session disconnect. The Department stated its government

furnished equipment is configured to automatically initiate a session lock after 15 minutes of user inactivity, automatically terminate a session after 30 minutes of logical session inactivity and require user re-authentication with cached credentials or personal identity verification following user session termination. It also stated it has made a risk-based assessment and subsequent configuration decision within the bounds of NIST, CISA and OMB to allow system-level activities, established by a virtual private network connection, to continue after strict user interactions have ended.

OIG Response

OIG will continue to monitor the Department's progress in implementing Recommendations 2.1, 2.3 and 2.6, and will validate the corrective actions taken during our FY 2021 FISMA audit fieldwork.

For Recommendation 2.2, OIG has already provided the list of Department websites that we identified as still using TLS 1.0 and 1.1. OIG agrees the Department needs to continue ensuring that all Department connections are migrated to TLS 1.2 or higher. However, the recommendation allows for the Department to develop enhanced controls to ensure all websites are migrated to the recommended TLS 1.2 protocol. Therefore, the Department needs to establish a corrective action plan to ensure that this issue is fully corrected in the future.

For Recommendation 2.4, OIG has already provided information to the Department regarding unsupported operating systems and outdated software that were identified during our system security assessment testing. OIG will provide further background information as necessary to assist the Department in validating the finding. We will validate the corrective actions taken for this recommendation during our FY 2021 FISMA audit fieldwork.

Regarding Recommendation 2.5, OIG considered the Department's response and did not revise the finding or recommendation. This is a repeat finding that has been identified during previous FISMA audits and resolved by OCIO. However, OIG testing validated that the issue continues to persist. Based on OIG testing, it validated that neither the system nor the user activity triggered a 30-minute timeout due to inactivity. Multiple tests were conducted that allowed OIG to remain connected over 1 hour without being disconnected by the session or connection. With regards to NIST 800-53, Rev 4, AC-12 (Session Termination), it states that the connection will terminate a session after a condition or triggered events require a session disconnect. Therefore, it appears that the trigger that should have disconnected the session that the Department referenced in its comments is not working as intended. OIG will need to conduct additional testing to validate what triggers are in place to terminate user sessions without terminating the network sessions.

Although the Department's response indicates that neither controls AC-12 nor SC-10 mandate specific timeframes or the use of user inactivity, OMB M-17-25 clearly states that "Remote connections timeout after 30 minutes of inactivity." To expand further, NIST SP 800-63B, Digital Identity Guidelines, proposes the following recommendation for providing high confidence for authentication—reauthentication of the subscriber shall be repeated following no more than 30 minutes of user inactivity. While the Department's government furnished equipment policy automatically initiates a session lock after 15 minutes of inactivity, during our testing, the sessions never terminated after 30 minutes of user inactivity. Consequently, a user that connects with a non-government furnished equipment computer will not be restricted by the policy enforcements and could be vulnerable to data leakage or data exposure. OIG agrees that there are situations when a system needs to stay connected to assure that software patches, configuration updates and other management processes take place. If the Department considers that a virtual private network connection is always an active connection, the concern is that the session will never terminate since the connection will continue to exist until the user terminates the session or connection.

In addition, OIG notes that the risk of an open connection on an unattended workstation largely depends on physical surroundings. A Department operated or managed office building may enforce strict physical controls for security. However, in a 100 percent telework status environment, when employees are not working in Department controlled space, the risk is higher that an unattended workstation could be compromised. As part of its corrective action plan, if the Department would like to formally accept the risk that inactivity is not specific to user activity because of its business needs and compensating controls the timeout requirement for its virtual private network session is appropriately mitigated, the OIG will consider the Department's actions during our FY 2021 FISMA audit.

METRIC DOMAIN 3—IDENTITY AND ACCESS MANAGEMENT

We determined that the Department's identity and access management program was consistent with the Defined level of the maturity model, which is considered not effective. 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.

Progress Made in FY 2020

We found the Department took several actions to improve its identity and access management program, especially in the areas of policies and procedures, roles and responsibilities and communications to stakeholders, encryption and authentication, remote access, and enterprise Identity, Credential, and Access Management (ICAM) solution.

Policies and Procedures
• developed, documented, and disseminated its policies and procedures for ICAM that have been tailored to the Department's environment; defined its ICAM strategy and developed milestones for how it plans to align with federal initiatives; 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; defined its processes for developing, documenting, and maintaining access agreements for individuals that access its systems; and defined its processes for provisioning, managing, and reviewing privileged accounts.
Roles and Responsibilities
• defined and communicated roles and responsibilities at the enterprise and information system levels for stakeholders involved in the ICAM program.
Encryption and Authentication
• planned for the use of strong authentication mechanisms for non-privileged and privileged users of the organization’s facilities, systems, and networks, including the completion of e-authentication risk assessments.
Remote Access
• ensured that end user devices have been appropriately configured prior to allowing remote access and restricted the ability of individuals to transfer data accessed remotely to unauthorized devices; configured all virtual private network remote access connections to require authentication along with a personal identity verification card; implemented the personal identity verification-alternate solution which allowed the Department to issue government furnished equipment laptops for new employees and contractors who did not have the ability to obtain physical personal identity verification cards from the Department or the General Services Administration due to the COVID-19 pandemic crisis.

Enterprise ICAM solution
• continued to rely on the ICAM program charter that established program authority to improve coordination, management, and oversight for the realization of the Federal ICAM program within the Department, which helped increase security, enforce compliance with laws and regulations, improve operability, enhance customer service, eliminate redundancy, and increase protection of personally identifiable information (PII); continued its efforts to transition to the enterprise ICAM solution, implemented in the development environment with the goal of activating the powerful enterprise tool by the end of 2020; planned for the ICAM solution to be fully integrated with the Department of Homeland Security's Continuous Diagnostics and Mitigation Program requirements, which will allow the Department to provide a single solution to address all of the requirements outlined in the OMB Memoranda M-19-17, "Enabling Mission Delivery through Improved Identity, Credential, and Access Management."

However, its practices in eight of the nine metric questions still do not meet the Managed and Measurable level 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 nine metric questions to achieve an effective Identity and Access Management metric domain. For example, the Department would need to completely transition to its desired ICAM architecture and integrate its ICAM strategy and activities with its enterprise architecture and the Federal Identity, Credentialing, and Access Management segment architecture.

Finding 3. 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 eight metric questions. Because the Department concurred with our 2019 recommendation to incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Identity and Access Management program, and agreed to complete this task by September 30, 2021, we did not reissue this recommendation for this year.

We determined that the Department's controls needed improvement for removing access of terminated users from the Department's network, improving controls over its password requirements, and configuring websites to display warning banners. This occurred because the Department was inconsistent with its implementation of the defined procedures, standards, and controls. As a result, this metric domain is considered not effective. An ineffective identity and access management program limits the Department's ability to identify users' and manage users access to its network resources properly and securely.

Department Did Not Consistently Enforce its own Password and Termination Standards

The Department did not consistently enforce its own password and account termination policy. As of July 2, 2020, the Department accounted for 15,315 accounts in its Active Directory. Out of the 15,315 accounts, 7,843 represented active accounts. Out of the 7,843 active accounts 7,096 represented accounts required to set a password, or with set password parameters to expire. Out of 7,096 active accounts, approximately 450 accounts did not change their password within the required 90-day timeframe. Also, approximately 109 accounts were not disabled after 90 days of inactivity, and approximately 168 account were not deactivated after 365 days of inactivity as required.

NIST SP 800-53, Revision 4, specifies that organizations are to enforce password minimum and maximum lifetime restrictions at the organization defined numbers for lifetime minimum, and maximum basis. In addition, the Department's latest adopted password standards, Standard PR.AC: Password Parameters, dated February 12, 2020, assigned the 90 days password lifetime for user and service accounts requiring that passwords must be changed after 90 days of use and requires deactivating all accounts with no activity after 365 days.

The Department did not adhere to its own standards enforcing passwords, terminations, and deactivations of its accounts. Without enforcing password policies, the Department's networks could be exposed to unauthorized users and compromise the confidentiality, integrity, and availability of information systems. In addition, terminated employees whose user accounts remained active with access to critical Department systems and resources increase the risk of unauthorized access by malicious users and compromise Departmental information resources.

Websites Not Configured to Display Warning Banners

We found that 43 of 572 websites were missing required login warning banners. The Department's corrective action to our FY 2018 recommendation stated that it would finish configuring all websites to display the required warning banners by October 31, 2019. However, during our FY 2020 audit fieldwork, we confirmed that although the Department closed the FY 2019 corrective action plan, this condition still existed. Specifically, our testing found that 43 websites failed to display the warning banners. The Department had previously communicated to its stakeholders, including FSA, that banners and acceptable text are to be in place by October 1, 2018. Although the Department developed a POA&M for the websites that had missing banners, it did not fully implement its October 2018 requirement. Further, Department policies and Federal guidance mandate a warning banner to alert users that they are accessing a government website.

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 system use notification, which requires organizations to 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. At minimum, warning banners should state that users should not expect any privacy when connecting to an IT asset owned and/or on behalf of the Department. Failure to display a banner could lead to individuals accessing government web resources without the warning label that outlines expectations in the login banner text; this could lead to disputes over appropriate access and use of data by the user and the government. We reported a similar condition in our FY 2017, 2018, and 2019 FISMA audits.

The Department's Controls Over Database Management Need Improvement

We performed database assessments for one of the eight systems judgmentally selected for testing during our audit, and identified vulnerabilities, configuration errors, and access issues. Specifically, the vulnerability scans identified significant security weaknesses that the Department needs to address to better safeguard data stored in the databases. Our scans of the database associated with this system identified 12 high vulnerabilities, 28 medium vulnerabilities, and 31 low vulnerabilities. Specifically, we found occurrences of (1) critical patching not performed; (2) security parameters not correctly set; (3) incorrect permissions, privileges, and roles assigned; (4) system table access not restricted to database administrators; (5) improper configurations; (6) failed login attempt parameters incorrectly set; (7) password parameters incorrectly set; and (8) unauthorized database links. Moreover, the Department had not consistently implemented the necessary controls to ensure that its databases were protected. We shared the vulnerabilities with the Department for remediation. By allowing these vulnerabilities to exist, the Department increases the risk that unauthorized individuals can access or alter its data. We reported similar conditions in our FY 2017, 2018, and 2019 FISMA audits.

Recommendations

We recommend that the Chief Information Officer require the Department to—

3.1 Establish oversight controls to ensure the Department's password, terminations, and deactivation policies are enforced accordingly.

3.2 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.[11] (Incorporates a Repeat Recommendation)

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

Department Comments

The Department concurred with Recommendation 3.1 and stated that it believes to have resolved the issue on September 9, 2020, based on notification from another ongoing OIG audit during August 2020. The Department will develop a corrective action plan by December 31, 2020, to address this recommendation.

The Department partially concurred with Recommendations 3.2 and 3.3. For Recommendation 3.2, it stated that at the time of the most recent OIG provided data regarding this finding, most websites that are currently without the required warning banner have a Risk Acceptance Form and POA&M in place. The Department will continue to monitor those POA&Ms and Risk Acceptance Forms in accordance with Department policies. Additionally, the Department explained that some of its components have variations of banners aligned with their authorities. Finally, some of the Department's vendors have indicated that segmenting traffic for banners would substantially increase costs by orders of magnitude as government customers use the same internet access points as commercial users. The Department will continue to monitor banner progress in FY 2021 and will develop a corrective action plan by December 31, 2020.

For Recommendation 3.3, the Department stated that based on the information provided by OIG at the time of this finding, most of the vulnerabilities found by were already covered under preexisting Risk Acceptance Forms and/or POA&Ms having been identified by the Department and treated through the Vulnerability Management program. Therefore, remediation plans and monitoring are in place. The Department will continue to monitor those POA&Ms and Risk Acceptance Forms in accordance with the Department's Vulnerability Management processes and procedures. For any remaining identified vulnerabilities, the Department will develop a corrective action plan by December 31, 2020.

[11] Recommendation 3.2 incorporates a repeat recommendation that the Department previously closed. However, our review identified that the finding remained; therefore, we reopened the recommendation so the Department can take further action to correct the problems identified.

OIG Response

OIG will continue to monitor the Department's progress in implementing Recommendation 3.1. We will review the corrective action plan to determine if the actions already taken will address the finding and recommendation and if so, will validate the corrective actions taken during our FY 2021 FISMA audit fieldwork.

For Recommendation 3.2, OIG agrees with the continuation of warning banner monitoring on all Department operated websites. OIG will review the corrective action plan to determine whether the actions will address the finding and recommendation and, if so, will validate them during our FY 2021 FISMA audit.

For Recommendation 3.3, OIG will review the corrective action plan and assess whether the actions will address the finding and recommendations during our FY 2021 FISMA audit fieldwork.

METRIC DOMAIN 4—DATA PROTECTION AND PRIVACY

We determined that the Department's data protection and privacy program was consistent with the Defined level of the maturity model, which is considered not effective. 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, or 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. 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.

Progress Made in FY 2020

We found the Department took several actions to improve its data protection and privacy program, especially in the areas of policies and procedures, roles and responsibilities, as well as data protection security controls and enhancements.

Policies and Procedures
• defined and communicated its privacy program plan and related policies and procedures for the protection of PII, data exfiltration and enhanced network defenses; defined and communicated its privacy awareness training program, including requirements for role-based privacy awareness training; in February 2020, published the "Standard ID.GV: Required Authorization Documentation" which included requirements for a Privacy Threshold Analysis (PTA) and a Privacy Impact Analysis (PIA).
Roles and Responsibilities
• consistently implemented its Data Breach Response plan by conducting a breach response table-top exercise and used lessons learned to make improvements to the plan; as part of the Department's reorganization efforts, the Department's Privacy Program was moved to the Office of Planning, Evaluation, and Policy Development, Student Privacy Policy Office, as such the Senior Agency Official for Privacy has remained in OCIO until a permanent Student Privacy Policy Officer Director is appointed.
Data Protection Security Controls and Enhancements
• established data protection security controls for least privilege users, data loss prevention solution, and use of encryption tools to prevent data exfiltration network defenses; expanded the data loss prevention system, an automated tool to monitor and prevent internal and external unencrypted email transmissions (including attachments), and web traffic from leaving the Department's boundary; expanded the Cybersecurity Risk Framework Scorecard to include privacy risks to further reinforce the integration of privacy into the Department's Cybersecurity Risk Management Framework and enabled Privacy Continuous Monitoring.

However, the Department's practices in all five areas still do not meet the Managed and Measurable level of maturity or an effective level of security. The Department would need to achieve a Managed and Measurable level on at least three of the five metric questions to achieve an effective Data Protection and Privacy metric domain. For example, the Department would need to ensure the enforcement of its policies and standards for PIAs, PTAs, and System of Records Notices (SORN). Finding 4 identifies the areas needing improvement for this metric domain in greater detail.

Finding 4. 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 Defined level for four metric questions. Because the Department concurred with our 2019 recommendation to incorporate additional measures to, at a minimum, achieve the Level 3 Consistently Implemented status of the Data Protection and Privacy program, and agreed to

complete this task by September 30, 2021, we did not reissue this recommendation for this year.

We determined that the Department was not consistently documenting PIAs, PTAs, or SORNs. This occurred because the Department's process for validating required privacy documentation was not fully implemented, nor consistently enforced for all of its Shareholders. As a result, this metric domain is considered not effective. 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. In addition, we identified other areas affecting data protection and privacy, which we address under other metric domains in this report.

The Department Did Not Consistently Document PIAs, PTAs, and SORNs

The Department was not consistently documenting PIAs, PTAs, or SORNs. To comply with Departmental and NIST guidelines, PTAs and PIAs must be signed and have a valid date within the previous 2 years, and be approved and signed by the Information System Security Officer, Information System Owner, and Chief Privacy Officer/Senior Agency Official for Privacy. Even though the Department established a process for the completion of PTAs and PIAs as part of required documentation for system security authorizations, it did not formally develop, nor implement a quality control review process until recently, to help ensure that PTAs, PIAs, and SORNS were up to date and complete. Moreover, the process was limited to biennial reviews and certifications of existing privacy documentation. Our testing of our eight judgmentally selected systems determined that (1) the Department did not complete a valid PTA for one system, (2) did not provide sufficient evidence for valid PIAs for two systems; and (3) did not complete a required SORN for one system. The Department did not have a consistent oversight process in place to validate and enforce the completion of PIAs, PTAs, and SORNs. By not consistently documenting and validating PIAs, PTAs, and SORNs as required, the Department cannot ensure that systems reflect most current privacy risks.

NIST SP 800-122, "Guide to Protecting Personally Identifiable Information," requires that PTAs be completed before the development or acquisition of a new information system and when substantial change is made to an existing system. In addition, the Department's Standard ID.GV: Required Authorization Documentation, dated February 12, 2020, specified that all systems must use the current version of the Department-approved PTA and to be valid, must be reviewed and signed by the Information System Owner and Privacy Safeguards Division every 2 years.

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 email transmission.

Recommendation

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

4.1 Establish additional processes, procedures, and monitoring controls to validate, track and enforce the completion of PIAs, PTAs, and SORNs.

Department Comments

The Department concurred with Recommendation 4.1 and will develop a corrective action plan by December 31, 2020, to address this recommendation.

OIG Response

OIG will continue to monitor the Department's progress in implementing Recommendation 4.1. We will review the corrective action plan to determine if the actions will address the finding and recommendation and if so, will validate the corrective actions taken during our FY 2021 FISMA audit fieldwork.

METRIC DOMAIN 5—SECURITY TRAINING

We determined that the Department's security training program was consistent with the Defined level of the maturity model, which is considered not effective. 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 information technology 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.

Progress Made in FY 2020

We found that the Department took several actions to improve its security training posture regarding policies, procedures, and standards; its enterprise-wide training

strategy; roles and responsibilities; assessment of knowledge, skills and abilities; and training comprehension testing.

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; developed the Standard PR.AT: Cybersecurity Awareness and Training, which established the Department standard for cybersecurity awareness and role-based training.
Enterprise-Wide Training Strategy
• consistently implemented an organization-wide security awareness and training strategy and plan; required new employees and contractors to participate in the Cybersecurity and Privacy Awareness training program before accessing the Department's network; and disabled accounts for employees and contractors who failed to take the Cybersecurity and Awareness trainings.
Roles and Responsibilities
• defined and communicated roles and responsibilities for security awareness and training program stakeholders across the organization.
Knowledge, Skills, and Abilities
• conducted an assessment of knowledge, skills, and abilities of its workforce to tailor awareness and specialized training; identified its skill gaps and began hiring focusing on the identified skill gaps.
Training Comprehension Testing
• conducted multiple phishing exercises across the organization.

Despite these actions, the Department's practices in all six areas still do not meet the Managed and Measurable level of maturity or an effective level 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 Security Training metric domain. For example, the Department would need to demonstrate that individuals with significant security responsibilities are provided specialized security training prior to information system access or performing assigned duties. Finding 5 identifies the areas needing improvement for this metric domain in greater detail.

Finding 5. The Department's Security Training Program Needs Improvement

We found that for the Security Training metric domain, the Department was at the Consistently Implemented level for three metric questions and Defined level for three metric questions. Because the Department concurred with our 2019 recommendation to incorporate additional measures to, at a minimum, achieve Level 3 Consistently

Implemented status of the Security Training program, and agreed to complete this task by September 30, 2021, we did not reissue this recommendation for this year.

We determined that the Department needed to improve its controls over the processes for ensuring new employees completed training before they received network access. This occurred because of the of Department's inconsistency in implementing its defined procedures. As a result, this metric domain is considered not effective. 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.

New Users Were Granted Network Access Before Completing Required Security Training

We found that the Department could not verify that all new users completed required security training before they accessed the Department's network. We received a list of 692 new user accounts that were created between October 1, 2019, and May 11, 2020. We judgmentally selected 10 new users (5 Department employees and 5 contractors) and determined 2 network accounts (1 Department employee and 1 contractor) were created prior to the user completing the Cybersecurity and Privacy Awareness training.

Although the Department established a standard operating procedure requiring new Departmental users to complete Cybersecurity and Privacy Awareness training before being granted a network account, it did not consistently implement the procedure. This also occurred for new contractor accounts being activated in the Department's Active Directory system. As a result, new users' network accounts were not restricted before the initial training requirement. If employees do not fulfill training requirements before accessing the network, the Department has no assurance that new users have appropriate knowledge to protect Department assets from compromise. We identified a similar condition in our FY 2017, 2018, and 2019 FISMA audits.

Although this condition was identified in past FISMA reports, OIG has noticed that by the decrease in occurrences we found in our audit fieldwork, the Department is making progress to strengthen its new employee and contractor security training process.

OMB Circular A-130, Appendix III, Management of Federal Information Resources, requires that all individuals be appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. In addition, the Department's Onboarding Process in ServiceNow, dated September 23, 2019, states that before submitting a request for a new user account, the new employee's Cyber Awareness Training Certificate must be attached to the request.

Follow-up on Prior Audit Role-Based Training Finding

In FY 2018, we found that the Department had not fully implemented a process for identifying and providing role-based training. According to the Audit Accountability and Resolution Tracking System, the corrective action was completed on July 27, 2020. The corrective action item stated that the requirement was incorporated as a process in the ICAM solution. Although incorporating the process into the ICAM solution closed out the action, as we identified in the Identity and Access Management metric area, that solution had not been fully implemented. Therefore, once the ICAM solution has been fully implemented, we can validate that the corrective action item was implemented. Because this corrective action item relies on recommendations identified in the Identity and Access Management metric area, we will not be making a separate recommendation in the Security Training metric area.

Recommendation

We recommend that the Chief Information Officer require the Department to—

5.1 Establish monitoring and oversight controls that ensure all new users satisfy all of the mandatory training requirements before they receive access to Departmental resources.[12] (Incorporates a Repeat Recommendation)

Department Comments

The Department partially concurred with Recommendation 5.1. The Department stated that it established processes to ensure that all employees and contractors complete mandatory Cybersecurity and Privacy Awareness Basics prior to system access. The Department disagrees that Security and Awareness Training, as a function, controls or owns the onboarding process of the Department's employees or contractors and the training program is an inappropriate mapping for this finding as it relates more closely to account provisioning and monitoring. Regardless, new employees and contractors are directed to complete their initial training using the Department's Security Touch learning management system; Federal Student Aid and the Institute of Education Sciences are authorized to provide awareness training to new contractors outside of Security Touch and training completed is documented via completion certificate. To validate completion of this requirement, monthly reports of new network accounts are compared against training records within the Department's learning management system. The Department stated that it can provide evidence of completion for all new

[12] Recommendation 5.1 incorporates a repeat recommendation that the Department previously closed. However, our review identified that the finding remained, therefore we reopened the recommendation so the Department can take further action to correct the problems identified.

users sampled as part of this report. For any remaining identified issues, the Department will develop a corrective action plan by December 31, 2020.

OIG Response

OIG considered the Department's response and subsequent evidence provided after the issuance of the draft report, and as a result revised the finding. However, Recommendation 5.1 was not revised. OIG acknowledges the Department's statements that it has established processes to ensure that all employees and contractors complete mandatory Cybersecurity and Privacy Awareness Basics prior to system access, however after several years of reporting this issue, the Department continues to fall short of consistently implementing this process. The recommendation allows for the Department to establish monitoring and oversight controls to ensure this process is consistently implemented; therefore, the Department needs to establish a corrective action plan to ensure that this issue does not occur in the future. The Department should submit additional evidence not already provided during the corrective action plan process for OIG to review and validate.

SECURITY FUNCTION 3—DETECT

The Detect security function comprises the *ISCM* metric domain. Based on our evaluation of the Department's ISCM program, we determined the Detect security function was consistent with the Defined level 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 in the Department's ability to fully implement the Department's ISCM strategy.

METRIC DOMAIN 6—INFORMATION SECURITY CONTINUOUS MONITORING

We determined that the Department's ISCM program was consistent with the Defined level of the maturity model, which is considered not effective. However, we identified areas where the Department made improvements to its ISCM program. 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.

Progress Made in FY 2020

We found that the Department took several actions to improve its ISCM posture regarding policies and procedures; roles and responsibilities; development of an enterprise-wide ISCM strategy; and metric collection and monitoring.

Policies and Procedures
• defined and communicated its ISCM policies and procedures, which is tailored to the Department's environment.
Roles and Responsibilities
• defined and communicated the structures of its ISCM team, with the ISCM stakeholders performing the roles and responsibilities that is defined across the organization.
Enterprise-Wide ISCM Function
• developed and communicated its ISCM strategy with all the required components; implemented its processes for performing ongoing security control assessments and granting system authorizations—including developing and maintaining system security plans and monitoring security controls; and, identified and defined performance measures and requirements to assess ISCM program effectiveness, achieve situational awareness, and control ongoing risk.
Metric Collection and Monitoring
• established a Continuous Monitoring Plan that defined ISCM metrics for hardware asset management, software asset management, configuration management settings, and vulnerability management; and developed a strategy for the collection and monitoring of all defined metrics to its operational systems with the use of Microsoft Power BI's reporting capabilities (including authorization status, POA&Ms, and Authorization to Operate documentation).

However, its practices in all five areas still did not meet the Managed and Measurable level of maturity or 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 ISCM metric domain. For example, the Department would need to demonstrate that its staff was consistently collecting, monitoring, and analyzing qualitative and quantitative performance measures across the organization and reporting data on the effectiveness of the organization's ISCM program. Finding 6 identifies the areas needing improvement for this metric domain in greater detail.

Finding 6. The Department's ISCM Program Needs Improvement

We found for the ISCM metric domain, the Department was at the Consistently Implemented level for two metric questions and Defined level for three metric questions. Because the Department concurred with our 2019 recommendation to incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the ISCM program, and agreed to complete this task by September 30, 2021, we did not reissue this recommendation for this year.

We determined the Department's controls needed improvement for fully implementing ISCM strategy and policies. This occurred because the Department did not monitor and consistently implement its defined processes. As a result, this metric domain is considered not effective. 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.

Department's ISCM Strategy Needs to be Updated to Reflect Current Environment

Although the Department developed and communicated its ISCM strategy inclusive of all required components and used a monthly Cybersecurity Framework Risk Scorecard to monitor and communicate high-level risks, it did not routinely review and update the strategy to reflect the current environment. The ISCM strategy is comprised of two documents—IAS-2 Detect and ISCM Roadmap. We inspected both documents to verify whether the Department's strategy supports the current ISCM processes and procedures. Specifically, the Department had not updated its ISCM strategy to reflect the current PIVOT environment. Based on our analysis, we found the ISCM strategy relies on draft documents that have not been approved, as well as outdated and discontinued policies and procedures. Furthermore, the Department did not properly monitor and perform reviews to determine any changes between the new, updated, or discontinued policy and procedures and the new PIVOT environment. Without an updated and accurate ISCM strategy in place that reflects the current environment and supporting processes, the Department would not be able to effectively implement processes to ensure ISCM program risks are identified and monitored.

According to the Standard Operating Procedure ED Cyber Security Policy Development, developed in March 2020, in the first quarter of the fiscal year, all IAS-developed Departmental cyber security policies (e.g., OCIO 3-112, five policy Instructions, Standards, and Job Aids) will undergo review to identify areas that need revision, update, or supplemental guidance. Once the annual policy review is complete, all relevant policies will be updated with, at minimum, a new signature date, and will be submitted to either the Chief Information Officer or the IAS Chief Information Security Officer for signature renewal.

Recommendation

We recommend that the Chief Information Officer require the Department to—

6.1 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.

Department Comments

The Department concurred with Recommendation 6.1. The Department stated that in the fourth quarter of FY 2020, it awarded a contract to evolve its ISCM program strategies and capabilities. Additionally, the Department will be updating all cybersecurity policies to reflect NIST SP 800-53, Revision 5, and its applicability to the current environment. The Department will continue these efforts in FY 2021 and will develop a corrective action plan by December 31, 2020.

OIG Response

OIG will continue to monitor the Department's progress in implementing Recommendation 5.1. We will review the corrective action plan to determine if the actions will address the finding and recommendation and if so, will validate the corrective actions taken during our FY 2021 FISMA audit fieldwork.

SECURITY FUNCTION 4—RESPOND

The Respond security function comprises the *Incident Response* metric domain. Based on our evaluation, we determined the Respond security function was at the Consistently Implemented level 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 reporting incidents to the United States Computer Emergency Readiness Team (US-CERT) and OIG needed improvement and data loss prevention (DLP) tools are not working as intended.

METRIC DOMAIN 7—INCIDENT RESPONSE

We determined that the Department's incident response program was consistent with the Consistently Implemented level of the maturity model, which is considered not effective. 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 (1) provide surveillance, situational monitoring, and cyber defense services; (2) rapidly detect and identify malicious activity and promptly subvert that activity; and (3) collect data and maintain metrics that demonstrate the impact of the Department's cyber defense approach, its cyber state, and cyber security posture.

Progress Made in FY 2020

We found the Department took several actions to improve its incident response program, especially in the areas of policies and procedures, roles and responsibilities,

incident response tools and technologies, and major transition of IT infrastructure and enhancements.

Policies and Procedures
• developed two new documents to support the consistent categorization and reporting criteria, the Incident Notification Guidelines and the Standard RS.CO: Computer Crime Incident Reporting; the Education Department's Security Operations Center updated its Incident Response Plan to assist in the new incident response activities; implemented the Standard PR.DS: PII Data Loss Prevention – Microsoft Office 365 detailing the minimum DLP requirements the Department must follow to prevent the intentional or accidental exposure of PII to unauthorized parties; defined a common threat vector taxonomy and developed handling procedures for specific types of incidents; defined its processes for reporting security incident information to US-CERT, law enforcement, Congress (for major incidents) and OIG; and, 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.
Roles and Responsibilities
• defined and communicated the structures of its incident response teams, roles and responsibilities of incident response stakeholders and those individuals who are performing the roles and responsibilities.
Incident Response Tools and Technologies
• participated in the deployment of Department of Homeland Security's EINSTEIN Intrusion Prevention Security Services on its network to identify traffic indicating known or suspected malicious cyber activity; utilized Einstein 3 Accelerated to detect and proactively block cyber-attacks or prevent potential compromises; expanded its DLP program, to identify, monitor, and automatically protect sensitive information across the entire Office 365 suite; utilized blocking of internet protocol addresses, or domains identified as being malicious; identified which internet service provider, business, or country the internet protocol address was registered in; and identified whether an internet protocol address or domain was blacklisted; and relied on Managed Trusted Internet Protocol Services for denial of service attacks.
Major Transition of IT Infrastructure and Enhancements
• Department went through a major transition of IT providers with the complete transition to the PIVOT contracts. As such, the Department updated its incident response policies, procedures, and supporting artifacts to support the change in provider technology and team structures.

However, its practices in six of the seven areas still did not meet the Managed and Measurable level of maturity or an effective level of security. The Department would need to achieve a 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 demonstrate that it used incident response metrics to measure and manage the timely reporting of incident information to its officials and external parties, and ensured data supporting the incident response metrics were accurate, consistent, and in a reproducible format. Finding 7 identifies the areas needing improvement for this metric domain in greater detail.

Finding 7. 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 one metric question, Consistently Implemented level for four metric questions, and the Defined level for two metric questions. We determined that the Department needed to improve controls for reporting incidents consistently to the US-CERT and OIG and ensuring data loss prevention tools worked as intended. This occurred because the Department did not consistently enforce its defined incident response and data safeguarding policies and standards. As a result, this metric domain is considered not effective. 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.

Department Did Not Comply with US-CERT and OIG Reporting Requirements

From October 1, 2019, through June 30, 2020, the Department accounted for 1,849 incidents and reportable events and 41 Department determined incidents. Out of the 41 Department determined incidents we noted 3 incidents that were not consistently reported in compliance with US-CERT reporting—with one taking over 12 hours, while another took 365 days to report.

For incidents reported late to US-CERT and/or OIG, we also identified misclassified categories and missing vector taxonomies, as well as inconsistent reporting of incidents and events to the OIG. Specifically, there were missing vector taxonomic elements such as current level of impact on agency functions or services. In addition, we identified incidents where an impact statement was not included. Likewise, none of the 41 Department determined incidents included scope of time and resources needed to recover from the incident.

For OIG reportable events—such as unauthorized access—one out of the three reported unauthorized access violations were reported. For exposure and release of PII violations being reported to OIG, we found instances where the violation was either not reported at all or only partially reported. In addition, the Department was not consistently reporting potential university breaches and was not consistently categorizing incidents.

For instance, we identified incidents that should have been categorized as scanning probing Category 5 yet coded as scanning probing under Category 3.[13] This occurred because the Department did not consistently monitor its incident response reporting requirements process. Despite the Department's capabilities to follow timely reporting, some of its processes remain manual which could cause validity and accuracy discrepancies for its incident reporting processes.

NIST SP 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," and NIST SP 800-61, Revision 2, "Computer Security Incident Handling Guide," provides several requirements for implementing an effective incident response program. Adhering to these requirements allows for establishing policies and procedures, implementing technical controls, and implementing and enforcing coordinated security incident activities. In addition, US-CERT Federal Incident Notification Guidelines specify that to clearly communicate incidents throughout the Federal Government and supported organizations, it is necessary for government incident response teams to adopt a common set of terms and relationships between those terms. All elements of the Federal Government should use this common taxonomy. Moreover, Department Standard RS.CO 1: Computer Crime Incident Reporting further clarifies that incidents that may constitute a computer crime (violations of applicable Federal and/or State laws) must be timely reported to the OIG.

Without an effective and efficient incident response program—one that is consistently implemented, used to measure and manage the implementation of the incident response program, achieve situational awareness, control ongoing risk, and adapt to new requirements and government-wide priorities—the Department increases the chance that it will be unable to detect a compromise to its IT systems. We identified similar issues in our FY 2017, 2018, and 2019 FISMA audits.

The Department Did Not Consistently Enforce its Computer Crime Incident Reporting Standards

The Department needs to improve its sharing of information on incident activities with internal stakeholders, such as OIG. Coordination with the OIG is governed by the "Standard RS.CO: Computer Crime Incident Reporting" (the Standard), issued in February 2020. Our review of the Standard found that it contains outdated and incorrect information and needs to be updated. For example, although the EDUCATE

[13] According to the Department's Incident Reporting Guideline, updated in March 2020, a Category 3 incident is classified as a successful installation of malicious software (i.e. virus, worm, etc.) that infects an operating system or application. A Category 5 incident is any activity that seeks to access or identify a Federal agency computer, open ports, protocols, service, or any combination for later exploit.

contract expired on July 31, 2019, the Standard still tasks the EDUCATE Contractor Security Personnel to evaluate the scans and steps involved to ensure that the threat has been mitigated. It also tasked EDUCATE with preparing and submission of a root cause analysis to the Chief Information Security Officer, Branch Chief of Cyber Security, and the Education Department Security Operations Center Coordinator. Moreover, we also noted that the version control of the document creates additional confusion, as some pages refer to Version 2.0, while others to Version 2.01. Finally, section 4.3 of the Standard is dedicated to containment, eradication, and recovery, and mandates that the Education Department Security Operations Center Coordinator is required to submit the root cause analysis to the OIG and share the results with the system owner. However, we confirmed with the OIG Technology Crimes Division that root cause analysis, or any other correspondence relevant to the root cause analysis, is not being submitted to OIG by the Education Department Security Operations Center.

The Department did not update its policy with the latest contractual obligations for incident eradication and adhere to its own reporting requirements to provide its stakeholders, OIG, with the actionable evidence. Without consistently enforcing effective and efficient incident response policies and providing actionable evidence to the law enforcement (i.e., OIG), the Department increases the chance that it will be unable to contain, and/or mitigate its incidents.

Data Loss Prevention Tool Did Not Function as Intended

The Department established a DLP process designed to help prevent the disclosure of PII or other sensitive data[14] and relied on a variety of tools[15] to detect and analyze these events. The Department expanded its DLP program with the release of Standard PR.DS: PII Data Loss Prevention – Microsoft Office 365 in May 2020. With a DLP policy integrated in the Office 365 Security and Compliance Center, the Department has the capability to identify, monitor, and automatically protect sensitive information across the entire Office 365 suite. The Department informed us that the Microsoft Office 365 DLP should have been operational starting in June 2020 and be able to detect and stop the transmission of unencrypted PII and Sensitive PII such as social security and credit card numbers. The Desktop DLP is still in a pilot and procurement stage, and the Network DLP is still in learning mode for fine tuning and enhancements.

[14] Sensitive information can include financial data or PII such as credit card numbers, social security numbers, or health records.

[15] These tools included the Office 365 Security and Compliance Center.

Our testing disclosed that DLP algorithms were not fully capable of detecting, blocking, or preventing transmission of unencrypted PII and Sensitive PII distributed to the external users. Rather, the solution is merely reacting to certain trigger words, and/or strings, and patterns of the actual content. For instance, the Department policy stipulates that DLP will block a credit card number if presented in a defined format. If the number is presented differently, the DLP does not detect it. We also verified that our testing efforts were not captured in the Education Department Security Operations Center incident report. The corrective action for this condition was closed out in Audit Accountability and Reporting Tracking System in April 2020. OIG testing confirmed the condition still existed in June 2020.

OMB and NIST guidelines identify several requirements for implementing an effective incident response program.[16] Adhering to the guidelines allows for establishing policies and procedures, implementing technical controls, and implementing and enforcing coordinated security incident activities.

DLP solution should be configured and applied consistently according to current policy to use multiple identifiers to assure that users are not able to bypass the DLP defenses. It is imperative to fine tune the solution capabilities to detect the suspicious activity and validate its configuration to disallow the transmission of PII and Sensitive PII over email. Without properly configured DLP algorithms, a malicious user and insider threat actor could circumvent the DLP defenses and exfiltrate massive amounts of data without being detected or stopped. As a result, public confidence in the Department's abilities to protect the PII could lead to data leakage, exposure, and serious damage to the Department's reputation.

Recommendations

We recommend that the Chief Information Officer require the Department to—

7.1 Incorporate additional measures to, at a minimum, achieve Level 4 Managed and Measurable status of the Incident Response program.

7.2 Develop and implement oversight controls to ensure that incidents are consistently submitted to US-CERT and the OIG within the required timeframes,

[16] OMB Memorandum M-14-03, "Enhancing the Security of Federal Information and Information Systems," November 2013; OMB Memorandum M-15-14, "Management and Oversight of Federal Information Technology," June 2015; NIST SP 800-53, Revision 4, "Recommended Security and Privacy Controls for Federal Information Systems and Organizations," April 2013; and NIST SP 800-61, Revision 2, "Computer Security Incident Handling Guide," August 2012.

are consistently categorized, and include the correct vector elements as required.

7.3 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.

7.4 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.[17] (Incorporates a Repeat Recommendation)

Department Comments

The Department partially concurred with Recommendation 7.1 and 7.3. For Recommendation 7.1, the Department believes it has achieved Level 4, Managed and Measurable maturity level for Incident Response because of its ability to use qualitative and quantitative measures to effectively monitor policies, procedures, and strategies that are collected and regularly updated. The Department stated that it has continued to enhance and improve on its ISP, to include efforts to improve its incident response capability through network access control enhancements, deployment of DLP, increased alerting around users traveling internationally with government furnished equipment without approval, operationalized Microsoft Office365 email security reporting, and completed updates/enhancements to 59 standard operating procedures. The Department will continue efforts to enhance qualitative methodologies to improve and better showcase the Department's incident response capabilities in FY 2021 and will develop a corrective action plan by December 31, 2020, to address this recommendation.

For Recommendation 7.3, the Department stated that the Education Security Operations Center monitors its incident response program on a continuous basis and the issues OIG identified were administrative errors. As part of continuous improvement efforts, updates/enhancements were made to 59 standard operating procedures and based on feedback from OIG Technology Crimes Division that the Education Security Operations Center was reporting too many incidents to OIG's Technology Crimes Division, efforts are underway to revise the Department's Computer Crimes Incident

[17] Recommendation 7.4 incorporates a repeat recommendation that the Department previously closed. However, our review identified that the finding remained, therefore we reopened the recommendation so the Department can take additional action to correct the problems identified.

Reporting Standard (RS.CO 1). Regarding the specific procedure referenced in this finding, the Department indicated that the wrong wording was incorporated to its policy and was missed during the standard operating procedure update effort, that referenced a vendor no longer operating at the Department. The Department will develop appropriate corrective action plans by December 31, 2020, to update the document.

The Department did not concur with Recommendations 7.2 and 7.4. For Recommendation 7.2, the Department stated that incidents are consistently submitted to US-CERT and the OIG and the issues identified with misreported incidents were administrative errors, which have been corrected. The Department stated these errors did not result in late reporting to US-CERT or the OIG. To identify and resolve administrative errors, including errors relating to incident time, date, and vector taxonomic elements, the Education Security Operations Center implemented a new quality control process to validate ticket accuracy at closure in August 2020.

For Recommendation 7.4, the Department stated its current DLP implementation (operational since October 9, 2019) is performing in accordance with established Department policy standards and that there are no current Federal mandates or directives requiring agencies to ensure DLP solutions are configured to a specific baseline beyond what is defined through agency-specific policy. The Department stated its current DLP capability enables it to identify and manage risks. It further states it conducts monthly DLP event reporting to identify trends and continuously measure the effectiveness of the rules in place. The Department stated it also provided education and guidance to users on how to secure transmission of PII or sensitive information and reinforces DLP requirements through the Cybersecurity Awareness Training program and Rules of Behavior.

OIG Response

OIG will continue to monitor the Department's progress in implementing Recommendations 7.1 and 7.3 and will validate the corrective actions during our FY 2021 FISMA audit.

For Recommendation 7.2, despite Department assurances that it consistently submitted all of its incidents to US-CERT and the OIG, and attributing the issues identified by the OIG to administrative errors, subsequent OIG validation will be conducted to ensure the errors were mitigated. OIG will also need to verify the newly established quality control process introduced to identify and resolve administrative errors, including errors relating to incident time, date, and vector taxonomic elements, as well as to validate that ticket accuracy was implemented and it is working as intended. During our audit, OIG provided the Department with multiple opportunities to update, correct, and clarify the incident report data, and as a result, OIG relied on the best available evidence to conduct its analysis with no indications from Department that the data provided

included erroneous entries. Therefore, although we recognize the proactive actions taken by the Department thus far to address our finding and recommendation, until independent validation is completed, the recommendation will remain unchanged.

Regarding Recommendation 7.4, the Department noted the lack of Federal mandates regulating DLP baseline. The NIST Special Publication 800-137.provides clear clarifications as to what an effective DLP strategy includes, such as data inventory and classification; data metric collection; policy development for data creation, use, storage, transmission, and disposal; and tools to monitor data at rest, in use, and in transit It further clarify that DLP tools have built-in detection and mitigation measures such as alerting via email, logging activities, and blocking transmissions. The Department further stated that its DLP solution is performing in accordance with established Department policy standards, and implied that the responsibility rests on its users. According to Department policy, the DLP settings must identify social security numbers and credit card numbers. However, OIG testing determined that the Department's DLP solution did not consistently perform in accordance with its policy. For instance, OIG testers were able to transmit hundreds of sensitive PII/PII outside of Department controlled networks without being detected. Specifically, OIG testers successfully transmitted to an external email address a test file containing 200 credit card numbers in a format that should have been blocked according to the Department's policy. Other testing confirmed that we were also able to avoid other policy blocking triggers by transmitting other files that contained anywhere from 10 to 200 unique records, and/or incorporating sensitive PII and PII. Our efforts were not an isolated case and should be addressed. Therefore, although we recognize the Department's commitment and improvements to its DLP solution, we believe continuous fine-tuning along with periodic testing is necessary to address our recommendation and minimize the exposure and potential reputational damage.

SECURITY FUNCTION 5—RECOVER

The Recover security function comprises 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 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. For instance, we found improvements were needed in the monitoring of the Department's contingency plan documentation.

METRIC DOMAIN 8—CONTINGENCY PLANNING

We determined that the Department's Contingency Planning program was consistent with the Consistently Implemented level of the maturity model, which is considered not

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

Progress Made in FY 2020

We found that the Department took several actions to improve its contingency planning posture regarding policies and procedures; roles and responsibilities; information system contingency plans; backup, storage, and recovery; and testing exercises.

Policies and Procedures
• consistently followed its defined information system contingency planning policies, procedures, and strategies; and updated its "Information System Contingency Planning Guidance" to include overall structure of contingency teams—including the hierarchy and coordination mechanisms and requirements among the teams, as well as updated the Recovery Time Objective and Recovery Point Objective determinations.
Roles and Responsibilities
• designated appropriate teams to implement its contingency plan strategies and assigned responsibility for monitoring and tracking the effectiveness of information systems continency plan activities; and consistently communicated information on the planning and performance of recovery activities to relevant stakeholders and executive management teams.
Information System Contingency Plans
• consistently implemented its process for ensuring that information system contingency plans are developed, maintained, and integrated with other contingency plans; updated Department's contingency plan template to align it with the Federal Risk and Authorization Management Program (FedRAMP) contingency plan template; and included elements such as establishing an alternate storage site, maintaining alternate storage agreements, maintaining information security safeguards equivalent to the primary site, and system backup frequency.
Backup, Storage, and Recovery
• consistently implemented its processes, strategies, and technologies for information system backup and storage—including the use of alternate storage and processing sites and performing backups of information at the user and system level.
Testing Exercises
• quarterly tabletop exercises for contingency planning and incident response were conducted.

However, the Department's practices in all seven areas still do not meet the Managed and Measurable level of maturity or an effective level of security. The Department would need to achieve a Managed and Measurable level of security for at least four of the seven metric questions to achieve an effective Contingency Planning metric domain. For example, the Department would need to ensure that its contingency plans were consistently updated and monitored. Finding 8 identifies the areas needing improvement for this metric domain in greater detail.

Finding 8. The Department's Contingency Planning Program Needs Improvement

We found that for the Contingency Planning metric domain, the Department was at the Consistency Implemented level for six metric questions and Defined level for one metric question. Because the Department concurred with our 2019 recommendation to incorporate additional measures to, at a minimum, achieve Level 4 Managed and Measurable status of the Contingency Planning program, and agreed to complete this task by September 30, 2021, we did not reissue this recommendation for this year.

We determined the Department did not consistently monitor and update its contingency planning information and needs to improve its monitoring of cloud service provider information system contingency planning controls. This occurred because the Department's processes were not consistently enforced, and were lacking proper validation and verification, policies and processes for its Cloud Providers. As a result, this metric domain is considered not effective. 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.

The Department Did Not Consistently Monitor and Update Its Contingency Planning Information

Although the Department established and maintained an enterprise-wide business continuity and disaster recovery program, we found that the Department did not consistently monitor and update its contingency planning information. Out of the eight judgmentally selected systems we evaluated, one system's disaster recovery plan was not current (last updated in 2017). We also identified one system that did not perform its annual contingency plan testing. In addition, for another system, the most recent disaster recovery tabletop exercise for one system took place in 2017. We further identified two Principal Office business continuity plans were not tested in FY 2020.[18]

[18] Institute of Education Services and Office of Finance Operations.

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 coordinating the contingency plan development and testing with organizational elements responsible for related plans. The Department's Standard ID.GV: Required Authorization Documentation, requires that contingency plan tests are to be performed on an annual basis and the current version of the information system contingency plan will be used to document the results of the annual contingency plan testing.

The Department did not consistently follow and enforce its own policies to ensure that plans are updated and tested as required. Without ensuring that the necessary planning and testing documentation is maintained and updated consistently, and that the plans contain all the required elements, the Department may not be able to successfully recover all of its IT resources in the event of a disaster.

The Department Needs to Improve its Monitoring of Cloud Service Provider Information System Contingency Planning Controls

The Department did not have a sufficient process for monitoring and verifying required information system contingency planning IT security controls and documentation of its cloud service providers. The Department's "Standard ID.GV: System Security Plan" Review assists the reviewers in assessing if a system's SSP meets the minimum Departmental requirements prior to system authorization. Furthermore, according to Department's Standard ID.GV: Required Authorization Documentation, in addition to documented evidence of information system contingency plans and annual test results, an approved SSP checklist is now required to be completed for a system to be authorized that must be updated annually. For all cloud service providers we reviewed, (EDAWSGov, EDAzureGov, EDServicenow, and EDAirwatch) an SSP checklist was completed and approved by the individual Information System Owners and Information System Security Officers, verifying that the cloud service provider or FedRAMP maintained these required documents available for review.[19] OIG obtained access to the

[19] FedRAMP provides processes, artifacts, and a secure repository that enables agencies to leverage authorization with standardized security requirements, conformity assessment identifying qualified independent, third-party security assessors, repository of authorization packages for secure clouds that all agencies can leverage, standardized ongoing assessment and authorization approach for Government clouds, standardized contract language to help agencies integrate FedRAMP requirements and best practices into acquisitions.

repositories of all four cloud service providers and could not locate the results of the contingency planning tests and disaster recovery plan tests.

After further review of the Department's documentation, we learned that all four cloud service providers' FedRAMP packages indicated that although contingency plan testing is performed annually, the test results are maintained outside of FedRAMP. According to Departmental guidance, in such instances, the anniversary date of the package authorization is used to meet requirements as the control is marked as implemented during an annual independent assessment review.[20]

NIST CSF Internal Controls, Information Protection, PR.IP-10, stated that the manager of network services and Chief Information Security Officer confirm that recovery plans are tested and they review results annually to ensure that the plan meets organization requirements. Also, NIST CSF Internal Controls, Supply Chain Risk Management, ID.SC-5, ensures that response and recovery planning and testing are conducted with suppliers and third-party providers.

Furthermore, the Department's Information System Contingency Planning Guidance, dated May 2020, requires that all contingency plan test and disaster recovery plan test results be documented in detail, reviewed, and uploaded into CSAM as evidence to support the required controls. Also, the fields for the completion date, as well as next due date or expiration date, must be updated in CSAM. We reviewed all four cloud service providers' information in CSAM and determined that three systems did not identify a disaster recovery plan test completion date.

The Department did not have an adequate process in place to validate and verify that its cloud service provider contingency planning controls were completed and documented before signing off on the SSP Checklists and prior to granting system authorizations. In addition, the Department was not consistent in following its process for updating CSAM with the required information fields. Without verification and validation of contingency planning test plans, the Department cannot ensure the successful recovery of operations and functionality of essential IT resources in the event of an emergency or service interruption.

[20] As per FedRAMP requirements, once the review of Security Package documents is complete for a given session, the agency must destroy and delete all copies of FedRAMP Security Package documents and not retain or publish them in any format.

Recommendations

We recommend that the Chief Information Officer require the Department to—

8.1 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.

8.2 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.

8.3 Establish additional procedures and controls to assure stakeholders are properly adhering to contingency planning guidance.

Department Comments

The Department partially concurred with Recommendations 8.1, 8.2, and 8.3. For Recommendation 8.1, the Department stated that it has invested in contract support to augment current Information System Security Officer support staff to manage system security planning more effectively. In the fourth quarter of FY 2020, the Department also enhanced the CSF Risk Scorecard and Security Documentation Status Report to incorporate business impact analysis, as well as disaster recovery planning and testing metric completion tracking across all applicable systems. The Department stated it will continue to utilize these reporting capabilities to provide more rigorous oversight in contingency planning activities and will develop a corrective action plan by December 31, 2020

For Recommendation 8.2 and 8.3, the Department again stated that it has invested in contract support to augment current Information System Security Officer support staff to enhance its system security planning processes. In the fourth quarter of FY 2020 the Department also stated that it enhanced the CSF Risk Scorecard and Security Documentation Status Report to incorporate all Department required authorization documents as metrics tracked for completion across all systems consistent with FedRAMP and NIST requirements. The Department stated that it does not believe additional controls or processes are necessary to confirm verification and validation of the contingency controls and that proper awareness of the existing processes and controls will be the focus of the Department's efforts. The Department stated that it will continue this effort in FY 2021 and will develop a corrective action plan to enhance Department policy to further clarify the Department's contingency planning requirements by December 31, 2020.

OIG Response

OIG will review the corrective action plans to determine whether the actions will address the finding and recommendations and, if so, will validate them during our FY 2021 FISMA audit.

For Recommendation 8.1, since the enhancements to the CSF Scorecard were made after our fieldwork ended, we were not able to review this information during the audit. OIG will validate this information and follow-up during our FY 2021 FISMA audit.

For Recommendations 8.2 and 8.3, OIG acknowledges the Department's statements that duplicative and additional controls would impact end users. However, our finding noted the current Department's process was insufficient and additional controls are needed to properly validate and verify that the cloud service provider contingency planning controls are completed and documented before signing off on the SSP Checklists and prior to granting system authorizations. Therefore, the Department needs to establish a corrective action plan to ensure that controls are in place and operating so does not occur in the future.

Other Matters. Policy Implementation and System Authorization Issue

Cybersecurity Policy Framework Implementation

As of May 2020, the Department is still in the process of implementing a new policy framework in alignment with the NIST Cybersecurity Framework and OMB M-17-25, "Reporting Guidance for Executive Order on Strengthening the Cybersecurity Federal Networks and Critical Infrastructure," issued on May 19, 2017. In December 2017, the Department initiated a Cybersecurity Framework Alignment for its policy and guidance. In March 2019, the Department's Chief Information Security Officer announced that as part of the Enterprise-wide Information Security Program initiative, the OCIO's IAS Division began replacing existing Departmental cybersecurity guidance with policies, instructions and standards that align to the NIST Cybersecurity Framework. This initiative began in October 2018, with issuance of the Department's overarching cybersecurity policy (OCIO 3-112), which superseded the prior policy, OCIO-01, Cybersecurity Handbook.

For FY 2020, there were no significant updates or changes to Departmental policies and procedures. The Department has not completely aligned all existing cybersecurity guidance to the NIST Cybersecurity Framework. With OCIO: 3-112 superseding OCIO-01, OCIO developed a document titled "OCIO-STND-01 Baseline Standard," issued February 13, 2020, which is based on OCIO-01 to bridge the gap ensuring all standards are aligned with the new policy. This document will remain valid until all the policies it contains have been absorbed into and superseded by supplementary standards.

We found that the Department has made improvements to its system authorization process and its policy creation. In October 2019, then subsequently updated in January and February 2020, OCIO developed the "Standard ID.GV: System Security Plan Review." This standard establishes the SSP review checklist, which assists the authorizing officials in assessing if an SSP meets the minimum Department requirements for signature. Additionally, in March 2020, OCIO developed the Standard Operating Procedure "ED Cyber Security Policy Development." This standard operating procedure establishes and centralizes a process for the development and revision of cyber security policy documents within the Department. IAS, under the guidance of the Branch Chief for Governance, Risk, and Policy, is now responsible for all cybersecurity policy documents. All new policies and policy updates are signed and authorized by the Chief Information Security Officer. Furthermore, the standard operating procedure details the Annual Policy review, which incorporates an annual review of all Departmental cyber security policies to identify areas that need revision, updates, or supplemental guidance.

Despite the efforts and initiatives the Department has taken to complete, review and align all cybersecurity policies to the NIST Cybersecurity Framework, more work is needed to ensure stakeholders are provided with clear instructions on protecting the Department information systems and data. During our review, we noted policy documents that contained incorrect information, even though they were approved and signed by the Chief Information Security Officer. For example, the PR.PT: Removable Media standard was referenced in OCIO-STND-01 that included a hyperlink. However, the PR.PT had not been published yet on the Department's Instructions and Standards website. Another example, the RS.CO: Computer Crime Incident Reporting standard, issued on February 12, 2020, still gives instructions to EDUCATE Contactor Security Personnel, while the EDUCATE contract officially came to an end on July 31, 2019.

The Department continues to demonstrate that it is engaged in updating guidance that will align with the NIST Cybersecurity Framework and that it will provide stakeholders with instructions on protecting the Department information systems and data. However, the Department still needs to continue to strengthen its cybersecurity development and review process to ensure the most accurate information is included in the policies, procedures, and/or standards for its stakeholders. We believe that if OCIO continues to incorporate the NIST Cybersecurity Framework into its policies and procedures and abides by its current policy and procedure process, it will better enable the Department to address current OIG findings, avoid future audit findings, and strengthen the Department's overall information security program.

AirWatch/Workspace ONE Authorization Issue

On June 10, 2020, 3 weeks before our end of fieldwork date, we were informed by OCIO officials about confusion and disconnect surrounding the transition of the Department's mobile device management solution from AirWatch to Workspace ONE. For most of our audit scope period, the Department used AirWatch for its mobile device management solution. AirWatch was one of the IT systems selected as part of our judgmental sample used for detailed testing and analysis throughout the FISMA audit metrics (see Appendix A).

AirWatch was replaced by Workspace ONE as the Department's mobile device management solution on February 24, 2020. The Department received the first communication from the vendor (VM Ware) of the transition on January 31, 2020, that stated the data center was being transitioned from AirWatch to Workspace ONE and that recipients of this correspondence should update their SSPs to reflect that agencies will now leverage VM Ware's Workspace ONE. In essence, this was considered as a new system as the Department's data was being transitioned from one data center to another, and the new data center was authorized under a different FedRAMP security package. The transition from AirWatch to Workspace ONE was fully completed on

February 24, 2020. OCIO officials informed us that on the original correspondence (January 31, 2020), not everyone impacted by the transition was notified. The communication was only distributed to one person and the email was not subsequently disseminated to the proper OCIO channels. Additionally, no further correspondence took place between the January 31, 2020 email, and the February 24, 2020 transition. Key stakeholders were not aware of the transition when it first happened and as a result were not able to register Workspace ONE in a timely fashion in CSAM.

In the months after, Workspace ONE received its Enterprise Architecture Review Board approval on April 23, 2020 and was registered in CSAM on April 24, 2020. The 2-month gap between the transition and this request was because of the failure of proper communication. AirWatch continued to remain operational in CSAM until May 19, 2020. This was done inadvertently because the Information System Security Officer from the OCIO Information System Security Branch was not notified of the transition until April 7, 2020. Once notified, the transition was briefed to the Chief Information Officer on April 8, 2020. Subsequently, AirWatch received Enterprise Architecture Review Board retirement approval on May 12, 2020, and was officially retired in CSAM on May 19, 2020.

As for the system authorization status of Workspace ONE, additional privacy information was requested by the Department's Senior Privacy Official before a full authorization would be granted. At the end of our fieldwork, Workspace ONE's Authorization to Operate was pending signature based on the additional information request of the Senior Privacy Official. A brief review of CSAM documentation revealed that Workspace ONE received its security authorization, via a signed Authorization to Operate, on August 4, 2020.

As a result, the Department's IT system responsible for its mobile device management solution was operating without proper authorization (approved Authorization to Operate) from February 24, 2020, until August 4, 2020, a total of 162 days. This occurred due to a lack of internal communication and information sharing between key stakeholders in OCIO.

Because the audit team was notified of this issue 3 weeks before our end of fieldwork date, there was not enough time to completely review system documentation and applicable Departmental policies and processes to validate the above information. However, OIG will review and follow-up on this issue during the FY 2021 FISMA audit fieldwork to determine if an underlying deficiency exists and how it can be rectified to prevent future instances from occurring.

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 2020, 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 eight metric domains associated with the security functions identified in the framework: (1) *Risk Management*, (2) *Configuration Management*, (3*) Identity and Access Management*, (4) *Data Protection and Privacy*, (5) *Security Training*, (6*) Information Security Continuous Monitoring*, (7) *Incident Response*, and (8) *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 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 2020 IG FISMA Metrics;
- reviewed and assessed FedRAMP cloud service provider security packages for select systems; and
- compared and tested management, operational, and technical controls based on NIST standards and Department guidance.

Additional testing steps to substantiate identified processes and procedures included the following:

- performed system-level testing for the *Risk Management*, *Configuration Management*, *Data Protection and Privacy*, and *Contingency Planning* metric domains;
- reviewed corrective action plans identified starting from January 2020 through July 2020;

- identified and verified systems that are routed through a trusted internet connection;
- tested websites for encryption protocols and login banners;
- tested and reviewed the Department's virtual private network protocols and solution;
- identified users who did not take required security training;
- reviewed computer security incidents that were reported from October 1, 2019, to June 30, 2020;
- reviewed access directory files ending July 2, 2020, to identify user, service, and machine accounts, as well as their compliance with password and termination policies and procedures;
- conducted a virtual walkthrough of the Education Department Security Operations Center to examine its capabilities and resources;
- performed vulnerability assessment testing on Department Amazon Web Services - Gov Cloud – IES Data Center, Department Amazon Web Services - Gov Cloud – TRIO Program Annual Performance Reports Data Collection and Processing Applications, Department Amazon Web Services - Gov Cloud – StudentHealth.gov, Education Central Automated Processing System, and Enterprise Technology Services - Infrastructure - General Support System;[21]
- verified security training evidence and completion;
- verified security settings for Department data protection; and
- observed the 2020 Department's disaster recovery tabletop exercise and test, which was conducted in a virtual setting.

We conducted our fieldwork from February 2020 through July 2020, primarily in a virtual setting due to the COVID-19 pandemic, but also at Department offices in Washington, D.C. We conducted an exit conference with Department and FSA officials on October 22, 2020.

[21] Due to the COVID-19 pandemic and no access to Department offices, we agreed to perform a limited security assessment testing for this year's FISMA audit in order 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 by the Department.

Sampling Methodology

As of January 2020, the Department identified an inventory of 116 systems that were FISMA reportable and classified as operational. Of the 116 FISMA reportable systems 2 were classified as high, 79 as moderate, and 35 as low-impact systems.

We primarily focused our system testing on Departmental systems due to the complete transition to the PIVOT environment, and our prior two FISMA audits focused almost exclusively on FSA systems. We judgmentally selected 8 of 34 Department systems that were non-FSA and had a Federal Information Processing Standards Publication 199 impact level of either high or moderate.[22]

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

[22] 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.

Table 3. Listing of Sampled Systems

Number	System Name	Principal Office	Impact Level
1	Department Amazon Web Services - Gov Cloud (EDAWSGov)	OCIO	High*
2	Department Azure - Microsoft Azure Government (EDAzureGov)	OCIO	High*
3	Education Security Tracking and Reporting System (EDSTAR)	OFO	Moderate
4	Education Central Automated Processing System (EDCAPS)	OFO	Moderate
5	Enterprise Technology Services - Infrastructure - General Support System (ETS-INFRA-GSS)	OCIO	Moderate
6	Department Airwatch - Airwatch by VMware Government Services (EDAirwatch)	OCIO	Moderate
7	Department ServiceNow – ServiceNow Service Automation Government Cloud Suite (EDServiceNow)	OCIO	Moderate
8	IES Data Center (IESDC)	IES	Moderate

*After we made our selection, we were notified that EDAWSGov and EDAzureGov was classified as High impact from FedRAMP, and after further analysis from OCIO, they were reclassified as Moderate in CSAM based on its operation within the Department's environment.

Testing of these systems helped us ascertain the security control aspects relating to *Risk Management*, *Configuration Management*, *Data Protection and Privacy* and

Contingency Planning.[23] In addition, some of these systems were the focus of our system vulnerability assessment and testing.

In addition to the sample of eight systems, we also used sampling to test certain aspects in the areas of *Risk Management*, *Configuration Management*, *Incident Response*, and *Security Training*. For *Risk Management*, we tested all of the 1,211 non-FSA POA&Ms for the timeframe of October 2017 through March 2020; all of the 1,751 FSA POA&Ms for the timeframe of October 2019 through March 2020; a judgmental sample of 6 IT contracts out of a total of 6,719 IT contracts/contract modifications; and a judgmental sample of 5 out of 71 users with non-compliant mobile devices. For *Configuration Management*, we tested all 623 Departmental websites for secure configurations for hypertext transfer protocol connection, encryption protocols, two-factor authentication, and login banners; inventory counts; and obsolete operating systems, applications, and databases.[24] For *Identity and Access Management*, we tested all 15,315 accounts contained in the Department's active directory. For *Security Training*, we tested a judgmental sample of 10 out of 692 new user accounts created from October 2019 through April 2020; we also tested a judgmental sample of 8 out of 3,541 employees and contractors that were required to complete role-based security training. For *Incident Response*, we tested all 1,890 incidents/events that occurred from October 2019 through June 2020. 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 vendor systems and applications externally hosted in a cloud environment. We used computer-processed data for the *Risk Management*, *Configuration Management, Identity and Access Management*, and *Security Training* 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

[23] 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.

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

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 FedRAMP'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 2019 and 2020)

Security Function	Metric Domain	FY 2019 Domain Maturity Level	FY 2020 Domain Maturity Level	FY 2019 Question Maturity Level	FY 2020 Question Maturity Level
Identify	Risk Management	Defined	Defined	• 10 at Defined • 1 at Consistently Implemented • 1 at Optimized	• 7 at Defined • ***4 at Consistently Implemented*** • 1 at Optimized
Protect	Configuration Management	Defined	***Consistently Implemented***	• 6 at Defined • 2 at Consistently Implemented	• 4 at Defined • 2 at Consistently Implemented • ***2 at Managed and Measurable***
Protect	Identity and Access Management	Defined	Defined	• 1 at Ad-hoc • 8 at Defined	• 8 at Defined • ***1 at Managed and Measurable***
Protect	Data Protection and Privacy	Defined	Defined	• 5 at Defined	• 4 at Defined • ***1 at Consistently Implemented***
Protect	Security Training	Defined	Defined	• 4 at Defined • 2 at Consistently Implemented	• 3 at Defined • ***3 at Consistently Implemented***
Detect	Information Security Continuous Monitoring	Defined	Defined	• 5 at Defined	• 3 at Defined • ***2 at Consistently Implemented***
Respond	Incident Response	Defined	***Consistently Implemented***	• 5 at Defined • 2 at Consistently Implemented	• 2 at Defined • ***4 at Consistently Implemented*** • ***1 at Managed and Measurable***
Recover	Contingency Planning	Consistently Implemented	Consistently Implemented	• 3 at Defined • 4 at Consistently Implemented	• 1 at Defined • ***6 at Consistently Implemented***

Note: Items in ***bold/italics*** highlight improvements from FY 2019 to FY 2020.

Appendix C. Status-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:

- For FY 2019, of the 37 recommendations made, 21 were reported as closed, and 16 remained open. Of the 21 closed recommendations, 9 were reopened because of our testing this year.
- For FY 2018, of the 45 recommendations made, 30 were reported as closed, and 15 remained open. Of the 30 closed recommendations, 2 were reopened because of our testing this year.

The tables below show the open, closed, and reopened recommendations from FY 2019 and 2018.[25]

FY 2019, OIG Audit Control Number A11T0002

Number	Recommendation	Status[a]	PCD/ACD[b]	OIG Determination
1.1	Incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Risk Management program.	Open	09/30/2021	Open
1.2	Ensure that POA&M remediation is performed within the required timeframe.	Open	09/14/2020	Open

[25] For FY 2017, the FISMA audit was officially closed out on March 12, 2020, in the Audit Accountability and Resolution Tracking System. Therefore, there were no open recommendations to report. Additionally, any closed recommendations that required reopening were encompassed in either the FY 2019 or 2018 recommendation determinations.

Number	Recommendation	Status[a]	PCD/ACD[b]	OIG Determination
2.1	Incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Configuration Management program.	Open	09/30/2021	Closed based on results from Metric Domain 2—*Configuration Management* of this report
2.2	Migrate to Transport Layer Security 1.2 or higher as the only connection for all Department connections.	Closed	07/27/2020	Reopened – See Finding 2 of this report
2.4	Ensure that 51 websites are routed through a trusted internet connection or managed trusted internet protocol service.	Open	02/28/2022	Open
2.6	Discontinue the use of unsupported operating systems, databases, and applications.	Closed	09/09/2020	Reopened – See Finding 2 of this report
3.1	Incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Identity and Access Management program.	Open	09/30/2021	Open
3.2	Ensure that terminated users' network access is removed timely.	Open	09/30/2020	Open
3.3	Ensure that access agreements for users accessing Department and FSA systems are documented and maintained. (Repeat Recommendation FY 2018 & FY 2019)	Open	09/30/2020	Open
3.4	Consistently document position risk designations for background investigations.	Open	09/30/2020	Open
3.5	Fully implement the Department's ICAM strategy to ensure that the Department meets full Federal government implementation of ICAM. (Repeat Recommendation FY 2018 & FY 2019)	Closed	07/27/2020	Reopened – See FY 2018 Recommendation 3.5 below
3.7	Validate the inactivity settings to ensure sessions time out after 30 minutes of inactivity.	Closed	02/04/2020	Reopened – See Finding 3 of this report
3.11	Require system owners configure all websites to display warning banners when users login to Departmental resources and ensure that banners include approved warning language by October 31, 2019.	Closed	01/23/2020	Reopened – See Finding 3 of this report

Number	Recommendation	Status[a]	PCD/ACD[b]	OIG Determination
4.1	Incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Data Protection and Privacy program.	Open	09/30/2021	Open
5.1	Incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Security Training program.	Open	09/30/2021	Open
5.2	Ensure that all new users complete the mandatory training requirements before they receive access to Departmental systems.	Closed	12/31/2019	Reopened – See Finding 5 of this report
5.3	Ensure that the process for ensuring completion of role-based training is fully implemented.	Closed	04/28/2020	Reopened but not reissued – Pending FY 2018 Recommendation 3.5 review
6.1	Require OCIO and FSA to incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the ISCM program.	Open	09/30/2021	Open
6.2	Automate its capabilities for monitoring the security controls effectiveness and overall implementation of the ISCM Roadmap. (Repeat Recommendation FY 2018 & FY 2019)	Open	10/30/2020	Open
6.3	Ensure the completion of Phases 1 and 2 of the Continuous Diagnostics and Mitigation program. (Repeat Recommendation FY 2018 & FY 2019)	Open	01/29/2021	Open
6.4	Require OCIO to implement a process that ensures data reported on the Cybersecurity Framework Risk Scorecard is accurate.	Open	09/30/2020	Open
7.1	Incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Incident Response program.	Open	09/30/2021	Closed based results from Metric Domain 7—*Incident Response* of this report
7.2	Require OCIO to ensure that incidents are consistently submitted to the OIG within the required timeframe.	Closed	06/03/2020	Reopened – See Finding 7 of this report

Number	Recommendation	Status[a]	PCD/ACD[b]	OIG Determination
7.3	Ensure that data loss prevention technologies work as intended for the blocking of sensitive information transmission.	Closed	04/02/2020	Reopened – See Finding 7 of this report
8.1	Incorporate additional measures to, at a minimum, achieve Level 4 Managed and Measurable status of the Contingency Planning program.	Open	09/30/2021	Open

[a] Status observed in the Audit Accountability and Resolution Tracking System as of September 14, 2020.
[b] If the status is marked open, the Planned Completion Date (PCD) is the date the Department indicated the recommendation will be closed. If the status is marked closed, the Actual Completion Date (ACD) is the date the Department indicated the recommendation was closed and action was taken.

FY 2018, OIG Audit Control Number A11S0001

Number	Recommendation	Status	PCD/ACD	OIG Determination
1.1	Incorporate additional measures to, at a minimum; achieve Level 4 Managed and Measurable status of the Risk Management program. (Repeat Recommendation from FY 2017)	Open	09/30/2021	Closed - Superseded by FY 2019 Recommendation 1.1
1.2	Ensure the completeness of individual corrective action plans for elements including remediation officials assigned, costs associated to remediate the weakness, and starting dates to remediate the weakness.	Closed	10/31/2019	Reopened – See Finding 1 of this report
1.3	Ensure that all contracts are reviewed and include all applicable privacy, security, and access provisions. (Repeat Recommendation from FY 2017)	Closed	03/25/2019	Reopened – See Finding 1 of this report
2.1	Incorporate additional measures to, at a minimum; achieve Level 3 Consistently Implemented status of the Configuration Management program. (Repeat Recommendation from FY 2017)	Open	09/30/2021	Closed based on results from Metric Domain 2—*Configuration Management* of this report
2.3	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
3.1	Incorporate additional measures to, at a minimum; achieve Level 3 Consistently Implemented status of the Identity and Access Management program. (Repeat Recommendation from FY 2017)	Open	09/30/2021	Open

Number	Recommendation	Status	PCD/ACD	OIG Determination
3.3	Enforce a two-factor authentication configuration for all user connections to systems and applications. (Repeat Recommendation from FY 2011, 2012, 2013, 2014, 2015, 2016 and 2017)	Open	02/01/2021	Open
3.5	Fully implement the Department's ICAM strategy to ensure that the Department meets full Federal Government implementation of ICAM. (Repeat Recommendation from FY 2017)	Open	12/31/2020	Open
4.1	Incorporate additional measures to, at a minimum; achieve Level 3 Consistently Implemented status of the Data Protection and Privacy program.	Open	09/30/2021	Open
5.1	Incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Security Training program. (Repeat Recommendation from FY 2017)	Open	09/30/2021	Open
6.1	Incorporate additional measures to, at a minimum; achieve Level 3 Consistently Implemented status of the ISCM program. (Repeat Recommendation from FY 2017)	Open	09/30/2021	Open
6.2	Automate its capabilities for monitoring the security controls effectiveness and overall implementation of the ISCM Roadmap. (Repeat Recommendation from FY 2017)	Open	10/30/2020	Open
6.5	Ensure the completion of Phases 1 and 2 of the Continuous Diagnostics and Mitigation program. (Repeat Recommendation from FY 2017)	Open	01/29/2021	Open
7.1	Incorporate additional measures to, at a minimum; achieve Level 3 Consistently Implemented status of the Incident Response program. (Repeat Recommendation from FY 2017)	Open	09/30/2021	Closed based on results from Metric Domain 7—*Incident Response* of this report
7.2	Ensure that incidents are consistently submitted to US-CERT and the OIG within the required timeframe and all incidents are consistently categorized. (Repeat Recommendation from FY 2017)	Open	10/30/2020	Open
7.3	Enable incident response tools and technologies to function on an enterprise basis.	Open	10/30/2020	Open

Number	Recommendation	Status	PCD/ACD	OIG Determination
8.1	Incorporate additional measures to, at a minimum; achieve Level 4 Managed and Measurable status of the Contingency Planning program. (Repeat Recommendation from 2017)	Open	09/30/2021	Open

Appendix D. CyberScope 2020 IG FISMA Metrics

For Official Use Only

Inspector General

Section Report

2020

Annual FISMA Report

Department of Education

For Official Use Only

Function 1: 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 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 - 4; FY 2020 CIO FISMA Metrics: 1.1 and 1.4, OMB A-130).

Defined (Level 2)

Comments: The U.S. Department of Education's Federal Information Security Modernization Act of 2014 for Fiscal Year 2020, Control Number ED-OIG/A11U0001 (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; NISTIR 8011; Federal Enterprise Architecture (FEA) Framework, v2; FY 2020 CIO FISMA Metrics: 1.2

Defined (Level 2)

Comments: ED-OIG/A11U0001 (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; NISTIR 8011; FEA Framework, v2; FY 2020 CIO FISMA Metrics: 1.2.5, 1.3.3, 3.10; CSF: ID.AM-2)?

Consistently Implemented (Level 3)

Comments: ED-OIG/A11U0001 (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 2020 CIO FISMA Metrics: 1.1; OMB M-19-03)?

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 1. The Department's Risk Management Program Needs Improvement.

Function 1: Identify - Risk Management

5 To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy, including for supply chain risk management. This includes the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk (NIST SP 800-39; NIST SP 800-53 Rev. 4: PM-8, PM-9; CSF: ID RM-1 - ID.RM-3; OMB A-123; OMB M-16-17; Green Book (Principle #6); CFO Council ERM Playbook; OMB M-17-25; NIST SP 800-37 (Rev. 2); NIST SP 800-161: Appendix E; CSF: ID.SC-1 - 2; SECURE Technology Act: s. 1326, Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain, May 15, 2019)?

Defined (Level 2)

Comments: ED-OIG/A11U0001 (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); OMB M-19-03; OMB M-15-14, FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-161; NIST SP 800-163, Rev. 1 CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?

Consistently Implemented (Level 3)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 1. The Department's Risk Management Program Needs Improvement.

7 To what degree have roles and responsibilities of internal and external stakeholders involved in risk management processes been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; OMB A-123; CFO Council ERM Playbook; NIST SP 800-37 (Rev. 2); OMB M-19-03)?

Defined (Level 2)

Comments: ED-OIG/A11U0001 (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); OMB M-19-03, CSF v1.1, ID.RA-6)?

Consistently Implemented (Level 3)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 1. The Department's Risk Management Program Needs Improvement.

Function 1: Identify - Risk Management

9 To what extent has the organization defined, communicated, and implemented its policies and procedures for conducting system level risk assessments, including for identifying and prioritizing (i) internal and external threats, including through use of the common vulnerability scoring system, or other equivalent framework (ii) internal and external asset vulnerabilities, including through vulnerability scanning, (iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities, and (iv) security controls to mitigate system-level risks (NIST SP 800-39; NIST SP 800-53 REV. 4: PL-2 and RA-1; NIST SP 800-30; CSF: Section 4.0; NIST SP 800-37 (Rev. 2))?

Consistently Implemented (Level 3)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 1. The Department's Risk Management Program Needs Improvement.

10 To what extent does the organization ensure that information about risks are communicated in a timely manner to all necessary internal and external stakeholders (CFO Council ERM Playbook; OMB A-123; OMB Circular A-11; Green Book (Principles #9, #14 and #15); OMB M-19-03; CSF: Section 3.3; SECURE Technology Act: s. 1326)?

Optimized (Level 5)

11 To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services (NIST SP 800-53 REV. 4: SA-4; NIST SP 800-152; NIST SP 800-37 Rev. 2; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4).

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 1. The Department's Risk Management Program Needs Improvement.

12 To what extent does the organization utilize technology (such as a governance, risk management, and compliance tool) to provide a centralized, enterprise wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123; CFO Council ERM Playbook)?

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 1. The Department's Risk Management Program Needs Improvement.

13.1 Please provide the assessed maturity level for the agency's Identify - Risk Management function.

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 1. The Department's Risk Management Program Needs Improvement.

Function 1: Identify - Risk Management

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

ED-OIG/A11U0001 (FISMA Report), Finding 1. The Department's Risk Management Program Needs Improvement.

Calculated Maturity Level - Defined (Level 2)

Function 2A: Protect - Configuration Management

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

Managed and Measurable (Level 4)

15 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)

16 To what degree have information system configuration management policies and procedures been defined and implemented across the organization? (Note: the maturity level should take into consideration the maturity of questions 17, 18, 19, and 21) (NIST SP 800-53 REV. 4: CM-1; NIST SP 800-128: 2.2.1)

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 2. The Department's Configuration Management Programs Need Improvement.

17 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 2020 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: ED-OIG/A11U0001 (FISMA Report), Finding 2. The Department's Configuration Management Programs Need Improvement.

18 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 2020 CIO FISMA Metrics: 2.1, 2.2, 2.14, 4.3; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1 and DE.CM-8)?

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 2. The Department's Configuration Management Programs Need Improvement.

Function 2A: Protect - Configuration Management

19 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 2020 CIO FISMA Metrics: 1.3.7, 1.3.8, 2.13, 2.14; CSF: ID.RA-1; DHS Binding Operational Directive (BOD) 15-01; DHS BOD 18-02)?

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 2. The Department's Configuration Management Programs Need Improvement.

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-19-26)

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 2. The Department's Configuration Management Programs Need Improvement.

21 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: ED-OIG/A11U0001 (FISMA Report), Finding 2. The Department's Configuration Management Programs Need Improvement.

22 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?

Cyberscope's calculated maturity level for Configuration Management was determined to be Defined (Level 2). However, based on our audit work, ED-OIG assessed the Configuration Management maturity level at Consistently Implemented (Level 3). See ED-OIG/A11U0001 (FISMA Report), Metric Domain 2 - Configuration Management.

Calculated Maturity Level - Defined (Level 2)

Function 2B: Protect - Identity and Access Management

Function 2B: Protect - Identity and Access Management

23 To what degree have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: AC-1, IA-1, and PS-1; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 3. The Department's Identity and Access Management Program Needs Improvement.

24 To what degree does the organization utilize an ICAM strategy to guide its ICAM processes and activities (FICAM)?

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 3. The Department's Identity and Access Management Program Needs Improvement.

25 To what degree have ICAM policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 26 through 31) (NIST SP 800-53 REV. 4: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; DHS ED 19-01; CSF: PR.AC-4 and 5)?

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 3. The Department's Identity and Access Management Program Needs Improvement.

26 To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate 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)?

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 3. The Department's Identity and Access Management Program Needs Improvement.

27 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 PS6)?

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 3. The Department's Identity and Access Management Program Needs Improvement.

Function 2B: Protect - Identity and Access Management

28 To what extent has the organization implemented strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800- 53 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.4 and 2.7; CSF: PR.AC-1 and 6; and Cybersecurity Sprint)?

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 3. The Department's Identity and Access Management Program Needs Improvement.

29 To what extent has the organization implemented strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800- 53 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; DHS ED 19-01; and Cybersecurity Sprint)?

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 3. The Department's Identity and Access Management Program Needs Improvement.

30 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 2019 CIO FISMA Metrics: 2.3 and 2.5; NIST SP 800-53 REV. 4: AC-1, AC-2 (2), and AC-17; CSIP; DHS ED 19- 01; CSF: PR.AC-4).

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 3. The Department's Identity and Access Management Program Needs Improvement.

31 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-17 and SI-4; CSF: PR.AC-3; and FY 2019 CIO FISMA Metrics: 2.10)?.

Managed and Measurable (Level 4)

32 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?

ED-OIG/A11U0001 (FISMA Report), Finding 3. The Department's Identity and Access Management Program Needs Improvement.

Calculated Maturity Level - Defined (Level 2)

Function 2C: Protect - Data Protection and Privacy

33 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); OMB M-18- 02; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J)?

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 4. The Department's Data Protection and Privacy Program Needs Improvement.

34 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 2019 CIO FISMA Metrics: 2.8; 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: ED-OIG/A11U0001 (FISMA Report), Finding 4. The Department's Data Protection and Privacy Program Needs Improvement.

35 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 2019 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5)?

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 4. The Department's Data Protection and Privacy Program Needs Improvement.

36 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 2018 SAOP FISMA metrics; OMB M-17-12; and OMB M-17- 25)?

Consistently Implemented (Level 3)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 4. The Department's Data Protection and Privacy Program Needs Improvement.

37 To what degree 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)? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements)

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 4. The Department's Data Protection and Privacy Program Needs Improvement.

Function 2C: Protect - Data Protection and Privacy

38 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?

ED-OIG/A11U0001 (FISMA Report), Finding 4. The Department's Data Protection and Privacy Program Needs Improvement.

Calculated Maturity Level - Defined (Level 2)

Function 2D: Protect - Security Training

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

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 5. The Department's Security Training Program Needs Improvement.

40 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: ED-OIG/A11U0001 (FISMA Report), Finding 5. The Department's Security Training Program Needs Improvement.

41 To what extent does the organization utilize a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to its culture? (Note: the strategy/plan should include the following components: the structure of the awareness and training program, priorities, funding, the goals of the program, target audiences, types of courses/material for each audience, use of technologies (such as email advisories, intranet updates/wiki pages/social media, web based training, phishing simulation tools), frequency of training, and deployment methods (NIST SP 800-53 REV. 4: AT-1; NIST SP 800-50: Section 3; CSF: PR.AT- 1).

Consistently Implemented (Level 3)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 5. The Department's Security Training Program Needs Improvement.

Function 2D: Protect - Security Training

42 To what degree have security awareness and specialized security training policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 43 and 44 below) (NIST SP 800-53 REV. 4: AT-1 through AT-4; and NIST SP 800-50).

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 5. The Department's Security Training Program Needs Improvement.

43 To what degree does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST SP 800-53 REV. 4: AT-2; FY 2019 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: ED-OIG/A11U0001 (FISMA Report), Finding 5. The Department's Security Training Program Needs Improvement.

44 To what degree does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures) (NIST SP 800- 53 REV. 4: AT-3 and AT-4; FY 2019 CIO FISMA Metrics: 2.15)?

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 5. The Department's Security Training Program Needs Improvement.

45.1 Please provide the assessed maturity level for the agency's Protect Function.

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 2. The Department's Configuration Management Programs Need Improvement. ED-OIG/A11U0001 (FISMA Report), Finding 3. The Department's Identity and Access Management Program Needs Improvement. ED-OIG/A11U0001 (FISMA Report), Finding 4. The Department's Data Protection and Privacy Program Needs Improvement. ED-OIG/A11U0001 (FISMA Report), Finding 5. The Department's Security Training Program Needs Improvement.

45.2 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?

Cyberscope's calculated maturity level for Security Training was determined to be Consistently Implemented (Level 3). However, based on our audit work, ED-OIG assessed the Security Training maturity level at Defined (Level 2). See ED-OIG/A11U0001 (FISMA Report), Metric Domain 5 - Security Training.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 3: Detect - ISCM

46 To what extent does the organization utilize an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organizationwide approach to ISCM (NIST SP 800-37 (Rev. 2); NIST SP 800-137: Sections 3.1 and 3.6)?.

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 6. The Department's ISCM Program Needs Improvement.

47 To what extent does the organization utilize ISCM policies and procedures to facilitate organization-wide, standardized processes in support of the ISCM strategy? ISCM policies and procedures address, at a minimum, the following areas: ongoing assessments and monitoring of security controls; collection of security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and reviewing and updating the ISCM strategy (NIST SP 800-53 REV. 4: CA-7, NISTIR 8011) (Note: The overall maturity level should take into consideration the maturity of question 49)?.

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 6. The Department's ISCM Program Needs Improvement.

48 To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: CA-1; NIST SP 800-137; CSF: DE.DP-1; and FY 2019 CIO FISMA Metrics)?.

Consistently Implemented (Level 3)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 6. The Department's ISCM Program Needs Improvement.

49 How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls (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); NISTIR 8011; OMB M-14-03; OMB M-19-03)

Consistently Implemented (Level 3)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 6. The Department's ISCM 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)?

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 6. The Department's ISCM Program Needs Improvement.

51.1 Please provide the assessed maturity level for the agency's Detect Function.

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 6. The Department's ISCM Program Needs Improvement.

Function 3: Detect - ISCM

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?

ED-OIG/A11U0001 (FISMA Report), Finding 6. The Department's ISCM Program Needs Improvement.

Calculated Maturity Level - Defined (Level 2)

Function 4: Respond - Incident Response

52 To what extent has the organization defined and implemented its incident response policies, procedures, plans, and strategies, as appropriate, to respond to cybersecurity events (NIST SP 800-53 REV. 4: IR-1; NIST SP 800-61 Rev. 2; NIST SP 800- 184; OMB M-17-25; OMB M- 17-09; FY 2018 CIO FISMA Metrics: 4.2; CSF: RS.RP-1; Presidential Policy Direction (PPD) 41)? (Note: The overall maturity level should take into consideration the maturity of questions 53 - 58).

Consistently Implemented (Level 3)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 7. The Department's Incident Response Program Needs Improvement.

53 To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-18-02; OMB M-16-04; FY 2019 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?

Consistently Implemented (Level 3)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 7. 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-18-02; CSF: DE.AE-1, PR.DS-6, RS.AN-4, and PR.DS- 8; and US-CERT Incident Response Guidelines)

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 7. 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: ED-OIG/A11U0001 (FISMA Report), Finding 7. The Department's Incident Response Program Needs Improvement.

Function 4: Respond - Incident Response

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-18-02; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 4; DHS Cyber Incident Reporting Unified Message)

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 7. 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-18-02; PPD-41).

Managed and Measurable (Level 4)

58 To what degree 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: ED-OIG/A11U0001 (FISMA Report), Finding 7. The Department's Incident Response Program Needs Improvement.

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

Consistently Implemented (Level 3)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 7. The Department's Incident Response Program Needs Improvement.

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?

ED-OIG/A11U0001 (FISMA Report), Finding 7. The Department's Incident Response Program Needs Improvement.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 5: Recover - Contingency Planning

Function 5: Recover - Contingency Planning

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

Defined (Level 2)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 8. The Department's Contingency Planning Program Needs Improvement.

61 To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and strategies, as appropriate (Note: Assignment of an overall maturity level should take into consideration the maturity of questions 62-66) (NIST SP 800-34; NIST SP 800- 161; CSF: ID.BE-5, PR.IP-9, and ID.SC-5).

Consistently Implemented (Level 3)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 8. The Department's Contingency Planning Program Needs Improvement.

62 To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-17- 09; FY 2019 CIO FISMA Metrics: 5.1; CSF:ID.RA-4)?

Consistently Implemented (Level 3)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 8. The Department's Contingency Planning Program Needs Improvement.

63 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 2019 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?

Consistently Implemented (Level 3)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 8. The Department's Contingency Planning Program Needs Improvement.

64 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 2019 CIO FISMA Metrics: 5.1; CSF: ID.SC-5 and CSF: PR.IP-10)?

Consistently Implemented (Level 3)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 8. The Department's Contingency Planning Program Needs Improvement.

65 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 2019 CIO FISMA Metrics: 5.1.1; and NARA guidance on information systems security records)?

Consistently Implemented (Level 3)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 8. The Department's Contingency Planning Program Needs Improvement.

Function 5: Recover - Contingency Planning

66 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)?

Consistently Implemented (Level 3)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 8. The Department's Contingency Planning Program Needs Improvement.

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

Consistently Implemented (Level 3)

Comments: ED-OIG/A11U0001 (FISMA Report), Finding 8. The Department's Contingency Planning Program Needs Improvement.

67.2 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?

ED-OIG/A11U0001 (FISMA Report), Finding 8. The Department's Contingency Planning Program Needs Improvement.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 0: Overall

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

Not Effective

Function 0: Overall

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.

·Do not include the names of specific independent auditors, these entities should be referred to as "independent assessor" or "independent auditor"

·The assessment of effectiveness should not include a list of ratings by NIST CSF Function-level, as these will already be included in the performance summary

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 Departments performance in accordance with Fiscal Year (FY) 2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics. Although the Department had several notable improvements in implementing its cybersecurity initiatives, its overall IT security programs and practices were not effective in all of the five security functions. We had findings in all eight metric domains, which included findings with the same or similar conditions identified in prior reports. We determined the Department's programs were consistent with (1) Level 2 - Defined, which is considered not effective for five domains: Risk Management, Identity and Access Management, Data Protection and Privacy, Security Training, and Information Security Continuous Monitoring; and (2) Level 3 - Consistently Implemented, which is considered not effective for three domains: Configuration Management, Incident Response, and Contingency Planning. For FY 2020, the Department has improved on several individual metric scoring questions from FY 2019, especially in the areas of Risk Management, Incident Response and Contingency Planning. The Department also demonstrated improvement in its processes from FY 2019 within several metric areas.

APPENDIX A: Maturity Model Scoring

Function 1: Identify - Risk Management

Function	Count
Ad-Hoc	0
Defined	7
Consistently Implemented	4
Managed and Measurable	0
Optimized	1
Function Rating: Defined (Level 2) Not Effective	

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	0
Defined	4
Consistently Implemented	2
Managed and Measurable	2
Optimized	0
Function Rating: Defined (Level 2) Not Effective	

Function 2B: Protect - Identity and Access Management

Function	Count
Ad-Hoc	0
Defined	8
Consistently Implemented	0
Managed and Measurable	1
Optimized	0
Function Rating: Defined (Level 2) Not Effective	

Function 2C: Protect - Data Protection and Privacy

Function	Count
Ad-Hoc	0
Defined	4
Consistently Implemented	1
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2) Not Effective	

Function 2D: Protect - Security Training

Function	Count
Ad-Hoc	0
Defined	3
Consistently Implemented	3
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3) Not Effective	

Function 3: Detect - ISCM

Function	Count
Ad-Hoc	0
Defined	3
Consistently Implemented	2
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2) Not Effective	

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	2
Consistently Implemented	4
Managed and Measurable	1
Optimized	0
Function Rating: Consistently Implemented (Level 3) Not Effective	

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	6
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3) Not Effective	

Maturity Levels by Function

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management	Defined (Level 2)	Defined (Level 2)	ED-OIG/A11U0001 (FISMA Report), Finding 1. The Department's Risk Management Program Needs Improvement.
Function 2: Protect - Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training	Defined (Level 2)	Defined (Level 2)	ED-OIG/A11U0001 (FISMA Report), Finding 2. The Department's Configuration Management Programs Need Improvement. ED-OIG/A11U0001 (FISMA Report), Finding 3. The Department's Identity and Access Management Program Needs Improvement. ED-OIG/A11U0001 (FISMA Report), Finding 4. The Department's Data Protection and Privacy Program Needs Improvement. ED-OIG/A11U0001 (FISMA Report), Finding 5. The Department's Security Training Program Needs Improvement.
Function 3: Detect - ISCM	Defined (Level 2)	Defined (Level 2)	ED-OIG/A11U0001 (FISMA Report), Finding 6. The Department's ISCM Program Needs Improvement.
Function 4: Respond - Incident Response	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	ED-OIG/A11U0001 (FISMA Report), Finding 7. The Department's Incident Response Program Needs Improvement.
Function 5: Recover - Contingency Planning	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	ED-OIG/A11U0001 (FISMA Report), Finding 8. The Department's Contingency Planning Program Needs Improvement.
Overall	Not Effective	Not Effective	

Appendix E. Acronyms and Abbreviations

CSAM	Cyber Security Assessment and Management
CSF	Cyber Security Framework
Department	U.S. Department of Education
DLP	Data Loss Prevention
EDUCATE	Education Department Utility for Communications, Applications, and Technology Environment
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act of 2014
FSA	Federal Student Aid
FY	Fiscal Year
IAS	Information Assurance Services
ICAM	Identity, Credential, and Access Management
ICT	Information and Communications Technology
ISCM	Information Security Continuous Monitoring
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIVOT	Portfolio of Integrated Value-Oriented Technologies
POA&M	Plan of Action and Milestones
PTA	Privacy Threshold Analysis
SORN	System of Records Notices
SP	Special Publication
SSP	System Security Plan
TLS	Transport Layer Security
US-CERT	United States Computer Emergency Readiness Team

Department Comments

UNITED STATES DEPARTMENT OF EDUCATION

DATE: October 28, 2020

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

Jason Gray Digitally signed by Jason Gray Date: 2020.10.28 18:11:28 -04'00'

SUBJECT: Response to Draft Audit Report
The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2020
Control Number ED-OIG/A11U0001

Thank you for the opportunity to review and comment on the draft 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) 2020 Draft Report, Control Number ED-OIG/A11U0001. 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 2020, the Office of the Chief Information Officer (OCIO) successfully transitioned information technology (IT) services to support the capacity of 100% telework in response to the COVID-19 pandemic. This transition was executed without impact or compromise to the Department Information Security Program (ISP) and allowed the Department to continue its important mission without interruption. OCIO also increased communications to Department users to regularly emphasize cyber vigilance as well as individual responsibilities for data protection and privacy while structuring simulated phishing exercises around the current threat landscape to keep Department employees educated and vigilant.

While the Department appreciates the work of the OIG on this audit, the Department believes that a number 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 Department does not concur with three of the 24 recommendations and has provided clarification in response to other recommendations by noting partial concurrence. The remaining recommendations (which includes those to which we partially concur) will be addressed through corrective action plans developed by OCIO and as agreed upon by your office.

Below are responses that address each recommendation in the draft report.

REPORTING METRIC DOMAIN No.1: RISK MANAGEMENT

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

OIG Recommendation 1.1: Establish oversight controls to ensure that POA&Ms [plan of action and milestones] are assigned with the required criticality impact levels and remediation is conducted within the required timeframes. (Incorporates a Repeat Recommendation)

Management Response: The Department partially concurs with this recommendation. The Department views criticality as being consistently and appropriately applied per the latest POA&M SOP (v 1.8 dated 20 February 2020). In section 4.4 it is noted; *The ISO will create a POA&M injection for any and all vulnerabilities that exceed the thresholds and follow the pre-POA&M and continuous monitoring POA&M workflows if applicable.* If the vulnerability is not remediated within the set threshold, then a POAM will be injected to be tracked and remediated within the scheduled completion date (SCD). User defined criticality is not used for scorecard oversight purposes as part of the Department's POA&M Management process. The Department leverages "control risk severity," which is a new term for Cyber Security Assessment and Management (CSAM) derived criticality. Additionally, each POA&M is automatically assigned a control risk severity based upon the National Institute of Standards and Technology (NIST) control associated with each POA&M. The Department utilizes its Most Valuable Progress (MVP) report to prioritize POA&M reduction and remediation efforts. This is covered within the Cybersecurity Framework (CSF) Risk Scorecard Standard Operating Procedure (SOP). The Department agrees remediation within established timeframes can be improved. The Department will develop a corrective action plan by December 31, 2020 to address the recommendation.

OIG Recommendation 1.2: Develop and implement a Department-wide Information and Communications Technology (ICT) supply chain risk management strategy to include the supply chain risk tolerance, acceptable supply chain risk mitigation strategies, and foundational practices.

Management Response: The Department partially concurs with this recommendation. Nearly all the Department's supply chain risk management (SCRM) ICT concerns relate to services. Based on the requirements from statutory law, executive orders and NIST, a Department-wide SCRM-ICT program was neither required nor cost effective until the "B" provision (August 2020) of the 2019 National Defense Authorization Act (NDAA) was required. Prior to the SECURE ACT, the Department had two systems needing SCRM support. Establishing a Department-wide program prior to the requirements of the SECURE Act would have been exceptionally costly and misaligned with the SCRM requirements of the time. The Department has re-assessed, and subsequently, re-categorized the two previous "High" impact systems to "Moderate" impact which removes NIST SP 800-53 Rev. 4 requirements to perform specific SCRM activities for High systems. However to meet the requirements of the NDAA Section 889, the Department has performed the following actions: established an Enterprise Risk Management Framework, which is fed by the Cybersecurity Risk Management Framework, both of which incorporate supply chain control risks where applicable; established an inter-agency agreement with the Department of Energy to utilize their operationalized enterprise SCRM program to help identify and reduce potential risks associated with third party vendor relationships; and, made additional investments in a new SCRM-ICT program support contract in the 4th Quarter. The Department is currently developing a Department-wide (vs. system specific) SCRM-ICT Program in alignment with the Department's established risk tolerance. The Department agrees opportunities exist to establish further supply chain risk reduction strategies in accordance with the Federal Acquisition Security Council (FASC). The Department will continue this effort in FY 2021 and will develop a corrective action plan by December 31, 2020 to address the recommendation.

OIG Recommendation 1.3: Develop a process to evaluate and routinely monitor supply chain risks associated with the development, acquisition, maintenance, and disposal of systems and products.

Management Response: The Department partially concurs with this recommendation. Nearly all the Department's SCRM-ICT concerns relate to services. Based on the requirements from law, executive orders and NIST, a Department-Wide SCRM-ICT program was not required nor cost-effective until the "B" provision (August 2020) of the 2019 NDAA was required. Prior to the SECURE ACT the Department had two systems needing SCRM support. Establishing a Department-wide program prior to the requirements of the SECURE Act would have been exceptionally costly and misaligned with the SCRM requirements of the time. The Department's acquisition processes include specific acquisition alerts requiring vendors to make representations regarding their adherence to SCRM. Furthermore, for SCRM matters issued through DHS or Cybersecurity and Infrastructure Security Agency (CISA) directives the Department developed procedures and instructions to ensure compliance with the requested actions. Additionally, the Department released Acquisition Alert (AA) 2019-03 "FAC 2020-03 and Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services for Equipment" and Acquisition Alert (AA) 2020-05, "Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment," requiring new federal and agency security requirements to address evolving threats specific to supply chain. OCIO has also awarded a new contract in the 4th Quarter of FY 2020 to further enhance the SCRM-ICT Program. The Department agrees further processes and procedures will be required as the FASC, Office of Management and Budget (OMB), and NIST provide further instructions and guidance regarding SCRM-ICT. The Department will develop a corrective action plan by December 31, 2020 to address the recommendation.

OIG Recommendation 1.4: Establish and automate procedures to ensure all Department-wide IT inventories are accurate, complete, and periodically tested for accuracy. Include steps to establish that all IT contracts are reviewed and verified for applicable privacy, security, and access provisions. (Incorporates a Repeat Recommendation)

Management Response: The Department partially concurs with this recommendation. Per the NIST Information System Component Inventory control CM-8 enhancement (2), the associated automation requirements apply to high systems, which do not apply to Department systems, as there are currently no high impact systems in our inventory. Hardware and software lists are required at the system level and monitored for completeness through the required authorization documentation risk factor in the daily CSF Risk Scorecard and Security Documentation Status Report. The Department agrees there are opportunities to improve the reconciliation of inventories between systems and external sources such as FedRAMP. The Department will continue this effort in FY 2021 and will develop a corrective action plan by December 31, 2020 to address the recommendation.

Regarding the security requirements in contracts, the Department disagrees. Five of the six contracts reviewed by the OIG, include provision 3452.239-72, which is enforceable language that addresses cybersecurity requirements outlined in Department standard ID.SC: Security and Privacy Languages for IT Contracts. One of the five contracts has the clause included in the blanket purchase agreement (BPA) and clauses flow down from the BPA to the respective task orders. Under BPA procedures, all task orders are subject to terms and conditions as defined within the BPA. The sixth contract is a simplified purchase of IT licenses with no services provided. Therefore, the requirements are not applicable. The Department continues to enforce cybersecurity and supply chain requirements through the Education Department Acquisition Regulations (EDAR) and acquisition processes. As contracts are formulated, they must comply with the EDAR and the subsequent cybersecurity and supply chain requirements. Through technical evaluation, contract proposals are reviewed to ensure vendors are proposing solutions that meet the Department's security requirements. Once awarded, the Contracting Officer's Representative (COR) and Contracting Officer (CO) work to ensure the cybersecurity requirements are being delivered

throughout the lifecycle of the contract in coordination with the associated Information System Security Officer (ISSO.)

OIG Recommendation 1.5: Verify and periodically reconcile the accuracy of cloud service provider inventories in or against CSAM.

Management Response: The Department partially concurs with this recommendation. As provided in the written responses to the Risk Management interview question number two, Department leveraged Cloud Service Providers (CSPs) are registered in CSAM, as the Department's official system of record for FISMA boundaries. We also provide the full list of Department authorized CSPs in other locations and formats to enable awareness for Department users and allow for rapid ingestion of available authorized CSP information. The official system of record, however, is CSAM and all derivative products must be reconciled with CSAM. The daily CSAM Data Discrepancies report was enhanced in the 4th Quarter of FY 2020 to monitor the CSP data field in CSAM to ensure accurate capture. The Department will continue to enhance quality assurance procedures to manage the CSP inventory more effectively across all applicable sources. This includes our current sources: CSAM (system of record), CSF Risk Scorecard, and CSP inventory derivatives as well as the FedRAMP PMO externally to ensure accurate capture across all sources. The Department agrees we have an opportunity to further enhance this process to ensure immutable evidence of reconciliation can be provided. We will develop a corrective action plan by December 31, 2020 to address the recommendation.

REPORTING METRIC DOMAIN No.2: CONFIGURATION MANAGEMENT

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

OIG Recommendation 2.1: Incorporate additional measures to, at a minimum, achieve Level 4 Managed and Measurable status of the Configuration Management program.

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2021 and will develop a corrective action plan by December 31, 2020 to address the recommendation.

OIG Recommendation 2.2: Develop enhanced oversight controls to ensure all Department connections are migrated to TLS 1.2 or higher cryptographic protocol. (Incorporates a Repeat Recommendation)

Management Response: The Department partially concurs with this recommendation. The Department conducts periodic scans and validation of our information systems and services to check for compliance to Transport Layer Security (TLS) version 1.2. Monthly vulnerability scans occur for external web sites as part of our continuous monitoring processes. In the event that a site is identified to be out of compliance, immediate outreach occurs to the Information System Owner (ISO) and ISSO and the issue is either resolved or a POA&M is created to monitor the resolution of the vulnerability in accordance with the Department's POA&M SOP. Finally, the Department's TLS and Forward Secrecy working group, established in FY 2020, meets regularly to review and prioritize remediation of impacted systems. While our data indicates we have effective oversight of TLS vulnerabilities, we agree that we need to continue ensuring that all Department connections are migrated to TLS 1.2 or higher. The Department will continue managing TLS risk in FY 2021. We welcome the OIG's test data for verification and validation, after which, we will develop a corrective action plan by December 31, 2020 to address the recommendation.

OIG Recommendation 2.3: Enhance implementation controls to prioritize and apply the most up-to-date and timely software patches and security updates to the identified systems and information technology solutions.

Management Response: The Department partially concurs with this recommendation. In FY 2020, the Department enhanced its Vulnerability Management (VM) program, complete with SOPs and guidance, to support the proper evaluation of vulnerability management and the unification of vulnerability management technology and programs across the Department's IT infrastructure. As part of oversight management controls, if identified vulnerabilities are unable to be remediated within the timeframe established in Department guidance, a POA&M is developed, monitored, and remediated through the Department's POA&M management process. The Department agrees vulnerability management controls should be enhanced on an ongoing basis in the balance of the mission, technology, and feasibility. The Department will develop a corrective action plan by December 31, 2020 to address the recommendation.

OIG Recommendation 2.4: Establish stronger monitoring controls to enforce the management of unsupported system components and track and discontinue the use of unsupported operating systems, databases, and applications. (Incorporates a Repeat Recommendation)

Management Response: The Department partially concurs with this recommendation. As a part of our IT modernization and migration to our new IT service providers, the software requirements in the contracts only allow for N-1 proposed solutions. N-1 means software, hardware or services can only be one version behind the current version. Additionally, an important consideration is the Department's ability to extend support for end of life or service system components by up to six months or longer depending on vendor. As a part of the Department's change and configuration management controls, identified unsupported system components are monitored and remediated through the Department's POA&M management process. We welcome the OIG's test results for verification and validation to determine if any of the items discovered are indeed not supported. When OIG provides the test and the results, the Department will develop a corrective action plan by December 31, 2020 to address the recommendation.

OIG Recommendation 2.5: Develop verification procedures and enforce the inactivity settings to ensure virtual private network (VPN) sessions time out after 30 minutes of inactivity. (Incorporates a Repeat Recommendation)

Management Response: The Department does not concur with this recommendation. OMB rescinded Memorandum M-07-16 that mandated the use of a "time-out" function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity; OMB M-17-25 requires the timeout of remote connections after 30 minutes of inactivity; neither memo specifies if user or system activity is the criteria for which the 30 minutes timeout applies. Furthermore, the FY 2020 Chief Information Officer (CIO) FISMA metrics, the most recent OMB and CISA requirements for FISMA Reporting, states "Percent (%) configured to time out after an organization defined risk-based period of inactivity and requires reauthentication to re-establish a session." regarding VPN configuration. Also, NIST Special Publication 800-53, Revision 4 control AC-12 addresses the termination of user-initiated logical sessions and control SC-10 addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions are terminated (and thus terminate user access) without terminating network sessions. Neither control AC-12 nor SC-10 mandate specific timeframes or the use of user inactivity. AC-12 permits the use of organization-defined conditions or trigger events requiring session disconnect while SC-10 permits the termination of the network connection associated with a communications session at the end of the session or after an organization-defined time period of

inactivity. The Department's Government Furnished Equipment (GFE) is configured to automatically initiate a session lock after fifteen minutes of user inactivity, automatically terminate a session after thirty minutes of logical session inactivity and require user re-authentication with cached credentials or personal identity verification (PIV) following user session termination. The Department has made a risk-based assessment and subsequent configuration decision within the bounds of NIST, CISA and OMB to allow system-level activities, established by a VPN connection, to continue after strict "user" (human) interactions have ended. For example, a session may stay connected (while locked) to complete critical processes and activities required to improve the security of the device, deploy patches, update configurations, perform e-discovery, optimize storage, and maintain accounts. We welcome validation of the OIG's testing and results for further reconciliation with our own.

OIG Recommendation 2.6: Correct or mitigate the vulnerabilities identified during the security assessment, in accordance with the severity level of each vulnerability identified.

Management Response: The Department concurs with this recommendation. As identified in information provided to the OIG after scanning results were reviewed by ISSOs, several of the vulnerabilities found were already covered under preexisting Risk Acceptances Forms (RAFs) and/or POA&Ms. The Department will continue to monitor those POA&Ms and RAFs in accordance with Department policies. The Department acknowledges there are opportunities to improve; however, all flaw remediation occurs in accordance with established policy and SOPs specific to VM and POA&M management. For any remaining identified vulnerabilities, the Department will develop a corrective action plan by December 31, 2020 to address the recommendation.

REPORTING METRIC DOMAIN No.3: IDENTITY AND ACCESS MANAGEMENT

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

OIG Recommendation 3.1: Establish oversight controls to ensure the Department's password, terminations, and deactivation policies are enforced accordingly.

Management Response: The Department concurs with this recommendation. The Department was notified of the issue through another ongoing OIG Audit in August 2020 and immediately took action to resolve the issue and believes to have resolved the issue on September 9, 2020. The Department will review the information provided as part of the FISMA audit to ensure that the measures that have been put in place have resolved the recommendation. The Department will continue this effort in FY 2021 and will develop a corrective action plan by December 31, 2020 to address the recommendation.

OIG Recommendation 3.2: 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)

Management Response: The Department partially concurs with this recommendation. At the time of the most recent OIG provided data regarding this finding most websites that are currently without the required warning banner have a RAF and POA&M in place. Additionally, any applicable laws which dictate or govern specific mandates should be considered as some components of the Department have variations of banners aligned with their authorities. The Department will continue to monitor those POA&Ms and RAFs in accordance with Department policies. Finally, some of the Department's vendors have indicated segmenting traffic for banners would substantially increase costs by orders of magnitude as government customers use the same internet access points as commercial users. The Department will continue to monitor banner progress in FY 2021 and will develop a corrective action plan by December

31, 2020 to address the recommendation regarding banner enforcement. We welcome the OIG's test data for verification and validation.

OIG Recommendation 3.3: Establish and enforce a corrective action plan to monitor and remediate identified database vulnerabilities.

Management Response: The Department partially concurs with this recommendation. As identified in information provided to the OIG; after system scanning, results are reviewed by ISSOs. Based on the information provided by OIG at the time of this finding, most of the vulnerabilities found by OIG were already covered under preexisting RAFs and/or POA&Ms having been identified by the Department and treated through the Vulnerability Management program. Therefore, remediation plans and monitoring are in place. The Department will continue to monitor those POA&Ms and RAFs in accordance with the Department's Vulnerability Management processes and procedures. Our analysis of the data provided by the OIG is ongoing and for any remaining identified vulnerabilities, the Department will develop a corrective action plan by December 31, 2020 to address the recommendation.

REPORTING METRIC DOMAIN No.4: DATA PROTECTION AND PRIVACY

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

OIG Recommendation 4.1: Establish additional processes, procedures and monitoring controls to validate, track and enforce the completion of PIAs, PTAs, and SORNs.

Management Response: The Department concurs with this recommendation. The Department will continue this effort in FY 2021 and will develop a corrective action plan by December 31, 2020 to address the recommendation.

REPORTING METRIC DOMAIN No.5: SECURITY TRAINING

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

OIG Recommendation 5.1: Establish monitoring and oversight controls that ensure all new users satisfy all the mandatory training requirements before they receive access to Departmental resources. (Incorporates a Repeat Recommendation)

Management Response: The Department partially concurs with this recommendation. The Department has established processes to ensure that all employees and contractors complete mandatory Cybersecurity and Privacy Awareness Basics prior to system access. However, the Department disagrees that Security and Awareness Training, as a function, controls or owns the onboarding process of the Department's employees or contractors. As such, the training program is an inappropriate mapping for this finding as it relates more closely to account provisioning and monitoring. Regardless, new employees and contractors are directed to complete their initial training using the Department's SecurityTouch learning management system; Federal Student Aid and the Institute of Education Sciences are authorized to provide awareness training to new contractors outside of SecurityTouch and training completed is documented via completion certificate. A copy of a Cybersecurity and Privacy Awareness Basics course completion certificate is provided to the Office of Finance and Operations, Personnel Security prior to the activation of a network account. To validate completion of this requirement, monthly reports of new network accounts are compared against training records within the Department's learning management system. The Department can provide evidence of completion for all new users sampled as part of this report. The Department welcomes verification of the OIG's testing and results. For any remaining identified issues,

the Department will develop a corrective action plan by December 31, 2020 to address the recommendation.

REPORTING METRIC DOMAIN No.6: INFORMATION SECURITY CONTINUOUS MONITORING

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

OIG Recommendation 6.1: Establish oversight controls to review, monitor and verify progress of the Information Security Continuous Monitoring (ISCM) strategy, as well as the annual reviews of all Departmental cyber security policies, to reflect the current environment.

Management Response: The Department concurs with this recommendation. In the 4th Quarter of FY 2020, the Department awarded a contract to evolve its ISCM program strategies and capabilities. Additionally, the Department will be updating all cybersecurity policies to reflect NIST SP 800-53 Rev. 5 and its applicability to the current environment. The Department will continue this effort in FY 2021 and will develop a corrective action plan by December 31, 2020 to address the recommendation.

REPORTING METRIC DOMAIN No.7: INCIDENT RESPONSE

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

Recommendation 7.1: Incorporate additional measures to, at a minimum, achieve Level 4 Managed and Measurable status of the Incident Response program.

Management Response: The Department partially concurs with this recommendation. The Department believes the evidence provided to the OIG, as mapped to the OIG FISMA Maturity Matrix, and further described in the responses to the recommendations below, that the Department has achieved Level 4, Managed and Measurable. The objective for Managed and Measurable is not that the Department had a perfect program with zero errors or abnormalities, but rather the Department's ability to use qualitative and quantitative measures to effectively monitor policies, procedures, and strategies are collected and regularly updated. The Department has continued to enhance and improve on its ISP, to include efforts to improve its incident response capability through network access control (NAC) enhancements and processes to notify the ED Security Operations Center (EDSOC) immediately upon alert, deployment of data loss prevention (DLP), increased alerting around users traveling internationally with GFEs without approval, operationalized O365 email security reporting, completed updates/enhancements to 59 SOPs, as part of ongoing continuous improvement efforts, SOPs are pulled and updated based on lessons learned from incident activities. The Department will continue efforts to enhance qualitative methodologies to improve and better showcase the Department's incident response capabilities in FY 2021 and will develop a corrective action plan by December 31, 2020 to address the recommendation.

Recommendation 7.2: Develop and implement oversight controls to ensure that incidents are consistently submitted to US-CERT and the OIG within the required timeframes, are consistently categorized, and include the correct vector elements as required.

Management Response: The Department does not concur with this recommendation. Incidents are consistently submitted to US-CERT and the OIG within the required timeframes with vector and taxonomy provided per CISA requirements. The issues identified with misreported incidents were administrative errors, which have been corrected and which upon further analysis had no significant impact to the risk or operations of the Department. Furthermore, these errors did not result in late reporting to US-CERT or the OIG. To identify and resolve administrative errors, including errors relating

to incident time, date, and vector taxonomic elements, the EDSOC implemented a new quality control process to validate ticket accuracy at closure in August 2020.

Recommendation 7.3: 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.

Management Response: The Department partially concurs with this recommendation. The EDSOC monitors its incident response program on a continuous basis and the issues identified were administrative errors. Updates/enhancements were made to 59 SOPs and as part of ongoing continuous improvement efforts, SOPs are pulled and updated based on lessons learned from incident activities. New SOPs were implemented, including one which increases alerting around users traveling internationally with GFEs without approval. OIG has full access to all incidents and tickets in real-time to review as they deem necessary. Based on feedback from OIG Technology Crimes Division (TCD) that the EDSOC was reporting too many incidents to OIG TCD, efforts are underway to revise the Department's Computer Crimes Incident Reporting Standard (RS.CO 1). Regarding the specific procedure referenced in this finding, the finding was around a single word, missed during the massive SOP update effort, that referenced a vendor no longer operating at the Department. The Department performed an analysis to determine if any incidents had been sent to the vendor due to the error in the document. Zero incidents had been sent and therefore the impact of the missed change in the document was zero. The Department will develop appropriate corrective action plans by December 31st, 2020 to update the document.

Recommendation 7.4: 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)

Management Response: The Department does not concur with this recommendation. The Department's current DLP implementation has been operational since October 9, 2019 and is performing in accordance with established Department policy standards and balancing the need for mission operations with the importance of security sensitive information. There are no current Federal mandates or directives requiring agencies to ensure DLP solutions are configured to a specific baseline beyond what is defined through agency-specific policy. The Department's DLP standard was designed to limit disruptions to legitimate mission and business operations while ensuring DLP capabilities operate without degrading system performance or preventing employees from performing their duties. The current DLP capability enables the Department to identify and manage risks associated with errors and omissions originating from non-malicious insiders and it is part of the Department's overall continuous monitoring solutions/processes in place to protect sensitive information. The Department has also operationalized monthly DLP event reporting to identify trends and continuously measure the effectiveness of the rules in place. Outcomes from this monitoring effort serve to influence any potential optimization and future enhancements to the Department's DLP policy, standard, and tool configuration. In FY 2020, the Department's DLP solution identified 11,198 potential DLP events, of which 9,809 were blocked. The remaining 1,389 events were overridden by the user as either false positives or justification exists. The EDSOC reviews all overrides to ensure the Department's policies were being followed. Through EDSOC's analysis, 1,153 were determined to be false positives while 236 were deemed business justifiable, zero were found to be abusing the DLP override capabilities. The Department has provided education and guidance to users on how to secure transmission of PII or sensitive information. Finally, the Department reinforces the DLP requirements through the Cybersecurity Awareness Training program, and the Department's Rules of Behavior which includes safeguarding personally identifiable information (PII). Training is conducted with annual completion requirements to maintain network access. Additionally, OCIO posts knowledge articles within the Intranet and the ServiceNow platform that provides users a how-to guide for using Department provided technologies for safeguarding PII

information to include encrypting PII information before sending to external stakeholders. We welcome validation and discussion of the OIG's test methods and results. However, at this time, our production data indicates the DLP function is operating in compliance with our standards as intended.

REPORTING METRIC DOMAIN No.8: CONTINGENCY PLANNING

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

Recommendation 8.1: 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.

Management Response: The Department partially concurs with this recommendation. In FY 2020, the Department has invested in ISSO contract support to augment current ISSO support staff to manage system security planning more effectively. In the 4th Quarter of FY 2020 the Department also enhanced the CSF Risk Scorecard and Security Documentation Status Report to incorporate business impact analysis, disaster recovery planning (DRP) and DRP testing as metrics tracked for completion across all applicable systems. The Department will continue utilizing these reporting capabilities to provide more rigorous oversight in contingency planning activities and will develop a corrective action plan by December 31, 2020 to address the recommendation.

Recommendation 8.2: 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.

Management Response: The Department partially concurs with this recommendation. In FY 2020, the Department has invested in ISSO contract support to augment current ISSO support staff to bolster system security planning processes. In the 4th Quarter of FY 2020 the Department also enhanced the CSF Risk Scorecard and Security Documentation Status Report to incorporate all Department required authorization documents as metrics tracked for completion across all systems consistent with FedRAMP and NIST requirements. The Department does not believe additional controls or processes are necessary to confirm verification and validation of the contingency controls. Duplicative and additional controls would be wasteful, redundant, and cumbersome for the end users. Rather, proper awareness of the existing processes and controls will be the focus of the Department's efforts. The Department will continue this effort in FY 2021 and will develop a corrective action plan to enhance Department policy to further clarify the Department's contingency planning requirements by December 31, 2020 to address the recommendation.

Recommendation 8.3: Establish additional procedures and controls to assure stakeholders are properly adhering to contingency planning guidance.

Management Response: The Department partially concurs with this recommendation. In FY 2020, the Department has invested in ISSO contract support to augment current ISSO support staff to bolster system security planning processes. In the 4th Quarter of FY 2020 the Department also enhanced the CSF Risk Scorecard and Security Documentation Status Report to incorporate all required authorization documents as metrics tracked for completion across all systems in accordance with FedRAMP and NIST requirements. The Department does not believe additional controls or processes are necessary to confirm verification and validation of the contingency controls. Duplicative and additional controls would be wasteful, redundant, and cumbersome for the end users. Rather, proper awareness of the existing processes and controls will be the focus of the Department's efforts. The Department will continue this effort in FY 2021 and will develop a corrective action plan to enhance Department policy to further

clarify the Department's contingency planning requirements by December 31, 2020 to address the recommendation.

Thank you for the opportunity to comment on this 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: Ann Kim, Deputy Chief Information Officer, Office of the Chief Information Officer
Mia Jordan, Chief Information Officer, Federal Student Aid
Wanda Broadus, Deputy Chief Information Officer, Federal Student Aid
Steven Hernandez, Director, Information Assurance Services, Office of the Chief Information Officer
Dan Commons, Director, Information Technology Risk Management Group, Federal Student Aid
Kelly Cline, 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