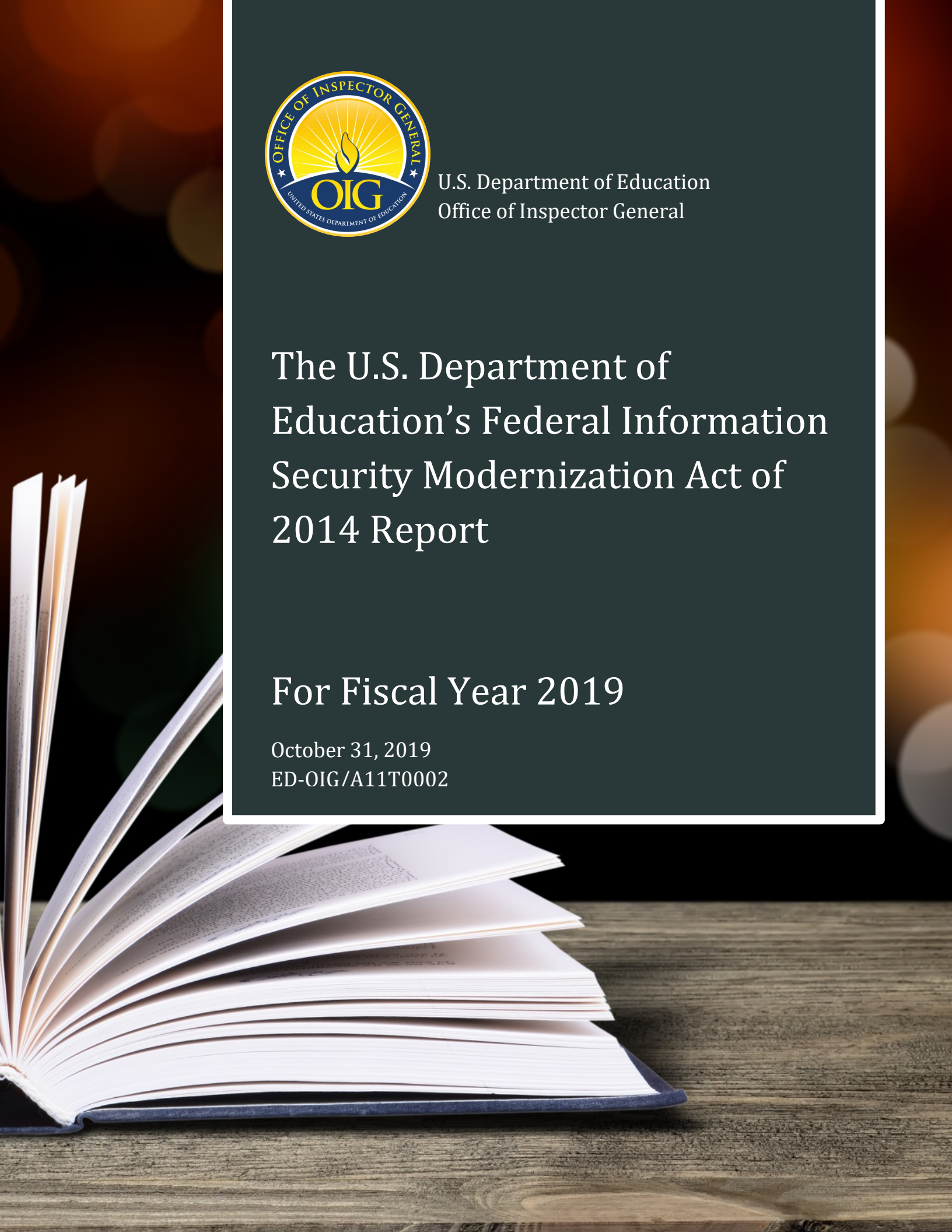

U.S. Department of Education
Office of Inspector General

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

For Fiscal Year 2019

October 31, 2019
ED-OIG/A11T0002

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 31, 2019

TO: Mitchell Zais, PhD
Deputy Secretary

Mark A. Brown
Chief Operating Officer

FROM: Robert D. Mancuso
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 2019
Control Number ED-OIG/A11T0002

Attached is the subject final audit report that covers the results of our review of the U.S. Department of Education's (Department) compliance with the Federal Information Security Modernization Act of 2014 for fiscal year 2019. An electronic copy has been provided to your Audit Liaison Officers. We received your comments on the findings and recommendations in our draft report.

Corrective actions proposed (resolution phase) and implemented (closure phase) by your offices will be monitored and tracked through the Department's Audit Accountability and Resolution Tracking System. The Department's policy requires that you develop a final corrective action plan for our review in the automated system 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.

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 six months from the date of issuance.

In accordance with the Freedom of Information Act (5 U.S.C. §552), reports issued by the Office of Inspector General are available to members of the press and general public to the extent information contained therein is not subject to exemptions in the Act.

We appreciate the cooperation given to us during this review. If you have any questions, please call Joseph Maranto at 202-245-7044.

Enclosure

cc:

Jason Gray, Chief Information Officer, Office of the Chief Information Officer
Ann Kim, Deputy Chief Information Officer, Office of the Chief Information Officer
Wanda Broadus, Acting 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
Mark Smith, Deputy Assistant Inspector General for Investigations
April Bolton-Smith, Post Audit Group, Office of the Chief Financial Officer
L'Wanda Rosemond, AARTS 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) and Federal Student Aid's (FSA) overall information technology security programs and practices were effective as they relate to Federal information security requirements. To answer this objective, we applied the Fiscal Year 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics (FY 2019 IG FISMA Metrics), which are grouped into five cybersecurity framework security functions that have a total of eight metric domains:

- **Identify** security function (one metric domain—Risk Management);
- **Protect** security function (four metric domains—Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training);
- **Detect** security function (one metric domain—Information Security Continuous Monitoring);
- **Respond** security function (one metric domain—Incident Response); and
- **Recover** security function (one metric domain—Contingency Planning).[1]

Specifically, we assessed the effectiveness of each security function using a maturity model approach developed as a collaborative effort among the Council of the Inspectors General on Integrity and Efficiency, the Office of Management and Budget, and the Department of Homeland Security. The maturity model comprises five maturity level scores: Level 1, Ad-hoc; Level 2, Defined; Level 3, Consistently Implemented; Level 4, Managed and Measurable; and Level 5, Optimized.[2] Level 1, Ad-hoc, is the lowest maturity level and Level 5, Optimized, is the highest maturity level. For a security function to be considered effective, agencies' security programs must score at or above Level 4, Managed and Measurable.

[1] These functions and metric domains are from the National Institute of Standards and Technology's "Framework for Improving Critical Infrastructure Cybersecurity." For more information, see the Background section.

[2] See Table 3 in the Background section for more information.

For the eight FY 2019 IG FISMA Metric domains, we assessed the effectiveness of security controls based on the extent to which the controls were implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information systems we reviewed in their operational environment.[3] Based on our work on these metric domains, we scored effectiveness against the maturity level reached within each of the five security functions.

Within each metric domain, we reviewed information technology controls, policies and procedures, and current processes, to determine whether they operated as intended as specified by the FY 2019 IG FISMA Metrics. We report our results on each of these metric domains to the Office of Management and Budget as required; see Appendix C.

Our audit work included the following testing procedures: (1) conducted system-level testing for the Configuration Management and Contingency Planning metric domains; (2) identified and verified systems required to use a trusted internet connection; (3) tested websites for encryption protocol; (4) tested active connection for security connection protocols; (5) reviewed computer security incidents; (6) performed vulnerability assessments of applications and databases; (7) verified training evidence and completion; and (8) verified security settings for Department data protection.

What We Found

We found the Department and FSA programs were not effective in any of the five security functions—Identify, Protect, Detect, Respond, and Recover. We also identified findings in all eight metric domains, which included findings with the same or similar conditions contained in prior Office of Inspector General reports.

At the metric domain level, we determined the Department's and FSA's programs are consistent with Level 2, Defined, for Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, and Incident Response. We also determined the Contingency Planning program is consistent with Level 3, Consistently Implemented. For a security function to be considered effective, agencies' security programs must score at or above Level 4, Managed and Measurable.

For FY 2019, the Department has improved on individual metric scoring questions. Specifically, we found the Department and FSA have improved their Security Training for

[3] Our determination of effectiveness is based on the definition cited in National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations."

two metric questions from Defined to Consistently Implemented; Identity and Access Management for one metric question from Ad Hoc to Defined; and Configuration Management for one metric question from Defined to Consistently Implemented.

The Department also demonstrated improvement from FY 2018 within several metric areas. For instance, in Configuration Management, the Department continues to decrease in the number of websites not enabling the use of encryption protocol. For Identity and Access Management, in December 2018, FSA issued its "Managing Privileged User Accounts" standard operating procedure for internally and externally hosted systems. For Data Privacy and Protection, the Department issued its Controlled Unclassified Information guidance, as well as fulfilled its annual requirement to perform its breach response tabletop exercise to discuss team roles during an emergency and team responses to an emergency or scenario.

However, the Department declined from FY 2018 within several metric areas. The most significant change was in Risk Management. Although the Department did not have any questions at the Ad Hoc level, it did decrease in the Optimized and Consistently Implemented levels resulting in 10 questions identified at the Defined level. As a result, the overall maturity rating for the security function went from Consistently Implemented to Defined. This was due to the new requirements in this year's FY 2019 FISMA IG Metrics addressing the SECURE Technology Act provisions for supply chain management, as well as related policy and procedural requirements such as imposing restrictions on the procurement and use of certain telecommunication equipment, software, and services from manufacturers owned, controlled, or connected to the Government of the People's Republic of China.

For Incident Response, question 57 declined from Managed and Measurable in FY 2018 to Consistently Implemented in FY 2019. This was due to (1) the low level of compliance with trusted internet connections; (2) the Portfolio of Integrated Value-Oriented Technologies transition Memorandum of Understanding was not complete; (3) the inconsistent communication and coordination with reporting incidents; and (4) Phase 1 and 2 of the Continuous Diagnostics Mitigation Federal Dashboard was not fully implemented.

For Contingency Planning, question 61 went from Managed and Measurable in FY 2018 to Consistently Implemented in FY 2019. This occurred because (1) a Business Impact Analysis was not consistently used to determine contingency planning requirements and priorities after a disaster; (2) the Department did not fully implement its information security continuous monitoring processes—including employing automated mechanisms to enhance its monitoring processes; and (3) the Department did not consistently implement its strategy regarding the collection and monitoring of all defined metrics for its operational systems. In addition, for Contingency Planning,

question 66 went from Managed and Measurable in FY 2018 to Consistently Implemented in FY 2019. As identified in tabletop exercises and after-action reports, monitoring and communication—especially with external shareholders—remains a challenge. Monitoring and communication were also identified as a challenge in the Incident Response metric. Except for Risk Management, the questions rated lower in FY 2019 did not impact the overall security function rating associated with these metric areas.

Table 1 shows the Department and FSA maturity level rating by domain and the number of questions by maturity level rating for fiscal years 2018 and 2019. We assessed the security program effectiveness using Maturity level ratings of Level 1, Ad-hoc; Level 2, Defined; Level 3, Consistently Implemented; Level 4, Managed and Measurable; and Level 5, Optimized. Level 1, Ad-hoc, is the lowest maturity level and Level 5, Optimized, is the highest maturity level.

Table 1. Metric Maturity Level Scores in Fiscal Years 2018 and 2019

Security Function	Metric Domain	FY 2018 Domain Maturity Level	FY 2019 Domain Maturity Level	FY 2018 Question Maturity Level	FY 2019 Question Maturity Level
Identify	Risk Management	Consistently Implemented	Defined	• 2 at 5 • 6 at 3 • 3 at 2 • 1 at 1	• 1 at 5 • 1 at 3 • 10 at 2
Protect	Configuration Management	Defined	Defined	• 1 at 3 • 7 at 2	• 2 at 3 • 6 at 2
Protect	Identity and Access Management	Defined	Defined	• 7 at 2 • 2 at 1	• 8 at 2 • 1 at 1
Protect	Data Protection and Privacy	Defined	Defined	• 5 at 2	• 5 at 2
Protect	Security Training	Defined	Defined	• 6 at 2	• 2 at 3 • 4 at 2
Detect	Information Security Continuous Monitoring	Defined	Defined	• 1 at 4 • 4 at 2	• 5 at 2
Respond	Incident Response	Defined	Defined	• 1 at 4 • 1 at 3 • 5 at 2	• 2 at 3 • 5 at 2

Security Function	Metric Domain	FY 2018 Domain Maturity Level	FY 2019 Domain Maturity Level	FY 2018 Question Maturity Level	FY 2019 Question Maturity Level
Recover	Contingency Planning	Consistently Implemented	Consistently Implemented	• 2 at 4 • 3 at 3 • 2 at 2	• 4 at 3 • 3 at 2

Although the Department and FSA made progress in strengthening their information security programs, we found areas needing improvement in all eight metric domains. Specifically, we found that the Department and FSA can strengthen their controls in areas such as its (1) remediation process for its Plan of Action and Milestones (Risk Management); (2) use of unsecure connections and appropriate application connection protocols (Configuration Management); (3) reliance on unsupported operating systems, databases, and applications in its production environments (Configuration Management); (4) protecting personally identifiable information (Configuration Management); (5) consistent performance of system patching (Configuration Management); (6) implementing the Identity, Credential, and Access Management strategy (Identity and Access Management); (7) implementing a process to manage privileged accounts (Identity and Access Management); (8) implementing two-factor authentication (Identity and Access Management); (9) removing access of terminated users to the Department's network (Identity and Access Management); (10) fully implementing its Continuous Diagnostics and Mitigation program (Information Security Continuous Monitoring); and (11) ensuring data loss prevention tools work accordingly (Incident Response). 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.

Our answers to the questions in the FY 2019 IG FISMA Metrics template, which will become the CyberScope report, are shown in Appendix C. In addition, we report on the status of the Department's program realignment and policy implementation in Appendix B.

What We Recommend

We made 37 recommendations (5 of which are repeat recommendations included in prior OIG reports) to assist the Department and FSA with increasing the effectiveness of their information security programs. The significant number of similar findings is due to prior year recommendations with corrective action plans due dates being outside of our audit timeframe. Full implementation of corrective action plans will help the Department and FSA 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.

The Department concurred with 31 recommendations, partially concurred with 4 recommendations, and did not concur with 2 recommendations. We summarized and responded to the Department and FSA's response at the end of each finding and included the full text of the Department and FSA's comments at the end of this report (see Department and FSA Comments). We considered the Department and FSA's comments, but did not make any changes to the report.

Introduction

Purpose

We performed this audit based on requirements specified by the Federal Information Security Modernization Act of 2014 (FISMA) and the Fiscal Year 2019 Inspector General FISMA Metrics V 1.3 (FY 2019 IG FISMA Metrics), issued on April 9, 2019. Our audit focused on reviewing the five security functions and eight associated metric domains: Identify (Risk Management), Protect (Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training), Detect (Information Security Continuous Monitoring), Respond (Incident Response), and Recover (Contingency Planning).

Background

The E-Government Act of 2002 (Public Law 107-347), signed into law in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act of 2002, the Federal Information Security Management Act of 2002, permanently reauthorized the framework established by the Government Information Security Reform Act of 2000, which expired in November 2002. The Federal Information Security Management Act of 2002 continued the annual review and reporting requirements introduced in the Government Information Security Reform Act of 2000, but it also included new provisions that further strengthened the Federal Government's data and information systems security, such as requiring the development of minimum control standards for agencies' systems. The Federal Information Security Management Act of 2002 also charged the National Institute of Standards and Technology (NIST) with the responsibility for developing information security standards and guidelines for Federal agencies, including minimum requirements for providing adequate information security for all operations and assets.

The E-Government Act of 2002 also assigned specific responsibilities to the Office of Management and Budget (OMB), agency heads, chief information officers, and inspectors general. It established that OMB is responsible for creating and overseeing policies, standards, and guidelines for information security and has the authority to approve agencies' information security programs. OMB is also responsible for submitting the annual Federal Information Security Management Act of 2002 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.

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, which must include the following:

- periodic risk assessments that consider internal and external threats to the integrity, confidentiality, and availability of systems, and to data supporting critical operations and assets;
- development and implementation of risk-based, cost-effective policies and procedures to provide security protections for the agency's information;
- training that covers security responsibilities for information security personnel and security awareness for agency personnel;
- periodic management testing and evaluation of the effectiveness of security policies, procedures, controls, and techniques;
- processes for identifying and remediating significant security deficiencies;
- procedures for detecting, reporting, and responding to security incidents; and
- annual program reviews by agency officials.

In December 2014, FISMA 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 authority for the Department of Homeland Security (DHS) Secretary to administer the implementation of such policies and practices for information systems.

FISMA requires the Office of Inspector General (OIG) to assess the effectiveness of the agency's information security program. FISMA specifically mandates that each evaluation under this section 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.

The Council of the Inspectors General on Integrity and Efficiency, OMB, and DHS developed the FY 2019 IG FISMA Metrics, in consultation with the Federal Chief Information Officer Council. The FY 2019 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," as shown in Table 2.

Table 2. Alignment of the Cybersecurity Framework Security Functions to the FY 2019 IG FISMA Metric Domains

Security Functions	FY 2019 IG Metric Domains	NIST Definitions
Identify	Risk Management	Develops the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training	Develops and implements the appropriate safeguards to ensure delivery of critical infrastructure services
Detect	Information Security Continuous Monitoring	Develops and implements the appropriate activities to identify the occurrence of a cybersecurity event
Respond	Incident Response	Develops and implements the appropriate activities to maintain plans for resilience and the restore any capabilities or services that were impaired due to a cybersecurity event
Recover	Contingency Planning	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

FISMA and the FY 2019 IG FISMA Metrics require the inspectors general 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. Table 3 details the five maturity model levels.: (1) Ad Hoc, (2) Defined, (3) Consistently Implemented, (4) Managed and Measurable, and (5) Optimized. Within the context of the maturity model, Levels 4 or 5 represent an effective level of security.[4]

[4] NIST SP 800-53, Revision 4, "Security and Privacy of Controls for Federal Information Systems and Organizations," defines security control effectiveness as the extent to which the controls are

Table 3. Level of Maturity and Description

Maturity Level	Maturity Level Description
Level 1: Ad-Hoc	Policies, procedures, and strategy are not formalized, and activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on changing threat and technology landscape and business/mission needs.

As described in the FY 2019 IG FISMA Metrics, ratings throughout the eight domains are by simple majority, where the most frequent level across the questions will serve as the domain rating. Further, inspectors general determine the overall agency rating and the rating for each of the Cybersecurity Framework Functions at the maturity level. Beginning in fiscal year (FY) 2009, OMB required Federal agencies and OIGs to submit FISMA reporting through the OMB Web portal, CyberScope (Appendix C).

Department's Information Technology Investments

The Department's FY 2019 total spending for information technology investments was estimated at $732 million, which included $53 million in a Portfolio of Integrated Value-Oriented Technologies (PIVOT) information technology investments. Also included in

implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing/mediating established security policies.

the Department's total information technology investment is $25 million for two Federal Student Aid (FSA) systems within the scope of the FY 2019 FISMA audit. Overall, FSA systems manage a $1.4 trillion student aid portfolio for 42.8 million recipients. In addition, FSA routinely manages approximately 24, 800 system users having privileged and non-privileged access to 62 internally and externally hosted systems.

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 information technology resources in a manner that is consistent with the requirements of the Clinger-Cohen Act of 1996,[5] FISMA, and OMB Memorandum A-130.[6] OCIO is responsible for implementing the operative principles established by legislation and regulation, establishing a management framework to improve the planning and control of information technology investments, and leading change to improve the efficiency and effectiveness of the Department's operations. OCIO monitors and evaluates contractor-provided information technology services through a service-level agreement framework and develops and maintains common business solutions that are required by multiple program offices.

In addition to OCIO, FSA has its own chief information officer, whose primary responsibility is to promote the effective use of technology to achieve FSA's strategic objectives through sound technology planning and investments, integrated technology architectures and standards, effective systems development and production support. FSA's Chief Information Officer core business functions are performed by three groups, the Application Development Group, the Enterprise Information Technology Management Group, and the Enterprise Information Technology Services Group.

Department Systems

The Education Department Utility for Communications, Applications, and Technology Environment contract (EDUCATE), was a 10-year performance-based contract that ended in November 2017. It moved the Department to a contractor-owned, contractor operated infrastructure service model for managing information technology supporting

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

[6] OMB Memorandum A-130 establishes a minimum set of controls to be included in Federal automated information security programs, assigns Federal agency responsibilities for the security automated information, and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123.

6,100 end-users nationwide. The Department's Information Technology Service's Re-Compete initiative established PIVOT which replaced EDUCATE. The re-compete initiative awarded services to vendors based on a multi-contract acquisition approach. This approach is designed to encourage and incentivize service providers to focus on high-quality customer service, new product innovation, flexibility in addressing new and changing requirements, and optimized cost versus benefit in the delivery of information technology services to the Department over the life of the contracts. The operational framework of the PIVOT structure includes (1) information technology services oversight, (2) prime integrator and end-user services, (3) hosting, (4) mobile devices, (5) printers, and (6) network.

The Department awarded and completed transition activities related to the re-compete of the EDUCATE contract on July 31, 2019. In addition, several PIVOT Phase 1 activities, such as the deployment of 6,500 workstations, 872 printing devices, and 78 new scanning devices, were completed. The Department also completed upgrades to workstations and deployment of "BigFix," an International Business Machines solution that provides remote control, configuration management, patch management, and software distribution.

FSA Systems

In 2014, FSA developed a high-level strategy resulting in three service delivery models—a hybrid cloud (combination of public and private cloud); implementation of a contractor-owned, contractor-operated data center facility for legacy systems; and mainframe operations. These solutions are designed to meet NIST and FISMA security controls; are monitored and managed through a single operations portal; provide real-time operations visibility from application to infrastructure to security; and include an applications-focused optimization for mainframe, traditional hosting, and hybrid cloud solution.

In 2016, FSA's Virtual Data Center contract with Dell Services Federal Group for a general support system to consolidate and operate many of its student financial aid program systems expired. An 11-year contract was subsequently awarded to Hewlett-Packard Enterprises Services, which proposed the Next Generation Data Center, located at its Mid-Atlantic data center in Clarksville, Virginia, and a recovery site located in Colorado Springs, Colorado.

The Mid-Atlantic Data Center is managed by DCX Technologies (a sub-contractor to Hewlett-Packard). The transition from the Virtual Data Center to the Next Generation Data Center occurred in phases during 2017 through migration waves. This began with

establishing an authorization to operate[7] for the Next Generation Data Center general support system, and followed with separate migration waves that included the (1) Foundation Wave, (2) SharePoint Wave, (3) Integrated Technical Architecture Wave, (4) Financial Management Service operations, (5) Free Application for Federal Student Aid Wave, and (6) eZ-Audit, Postsecondary Educational Participant System, and eApp operations. The decommissioning of the Virtual Data Center site was completed November 2018.

Fiscal Year 2018 FISMA Audit Results

During last year's FISMA audit, we identified 8 findings and provided 45 recommendations that addressed the conditions noted in the report. The Department concurred with 39 recommendations, partially concurred with 4, and did not concur with 2. In general, our findings identified:

- outdated policies and procedures;
- unauthorized and unsecure connections to the Department's network;
- reliance on unsupported systems, databases, and applications;
- privileged system user accounts not properly managed;
- personally identifiable information not being protected;
- external network connections not using two-factor authentication;
- insufficient implementation of a network access control solution;
- an insufficiently implemented information security continuous monitoring program; and
- an insufficiently implemented incident response program.

The Department and FSA agreed to corrective actions such as reviewing acquisition packages for cybersecurity requirements and causes, providing immediate notification to stakeholders to mitigate and resolve identified vulnerabilities, updating policies and procedures, updating the Identity, Credential, and Access Management (ICAM) Roadmap and Implementation Plan, establishing cybersecurity workforce development documents, communicating issues through Risk Management Workshops, and

[7] The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations.

developing an Incident Response Maturity Model. As of July 2019, the Department and FSA reported that they had completed corrective actions for 12 of the 45 recommendations. The Department and FSA are scheduled to complete the remaining corrective actions by October 31, 2019, with some extending out as far as September 2021.

Audit Results and Findings

We identified 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 2011 through 2018.

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. The Department and FSA continue to develop and strengthen their risk management program. However, we noted that improvements were needed in the Department and FSA's corrective action plan remediation process, and in enforcing and monitoring inclusion of the required contract clauses.

METRIC DOMAIN 1—RISK MANAGEMENT

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

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 risk once it is determined, 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.

The Department established policies, procedures, roles, and responsibilities for system level risk assessment and security control selections that were consistent with NIST standards and communicated them across the organization.

The Department relied on the Cyber Security Assessment and Management tool as the official system of record for system documentation and inventory of all Department and FSA systems. The tool also incorporates the Risk Management Framework to provide system owners and other shareholders with the capabilities of addressing all six steps of the Risk Management Framework (including categorization and monitoring).

The Department used an enterprise-wide Cybersecurity Framework Risk Scorecard, published monthly, to communicate the Department's risks to all its stakeholders. The Department also implemented the scorecard in August 2017 and used it to perform regular framework-based risk assessments, identify gaps and improvement opportunities, enhance incident response capabilities, and to better protect its network assets and data. The scorecard considers system impact across the enterprise level, and includes a ranking of low, moderate, or high for all Departmental systems.

The Department relied on its Enterprise Risk Management Program to document its overarching risk management strategy. As part of its risk management process, the Department also coordinated with the Cyber Risk Council and included the Chief Financial Officer/Risk Officer in developing an overall risk strategy. In addition, FSA provided input into prioritizing enterprise-wide cyber risk. The Department also established a Risk Management Council with the goal to ensure that its risk strategy is implemented across the FSA enterprise. We also found that the Cybersecurity Framework Risk Scorecard was aligned with the risk identified in the Enterprise Risk Management program.

The Department used meetings, workshops, and monthly Cybersecurity Framework Scorecards to communicate risks by informing overall cybersecurity strategic planning at the Department level, enabling strategic planners to view, understand, and manage cybersecurity risk. This also helped internal and external stakeholders align cybersecurity activities with business requirements, risk tolerance, and resources. This was demonstrated through the Department's Quarterly Cybersecurity Risk Management workshops, the FY 2019 Cybersecurity Forums, and distribution of the Cybersecurity Framework Scorecard to stakeholders.

The Department relied on DHS' Continuous Diagnostics and Mitigation (CDM) program to identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. For sections of the CDM program, such as, CDM Defend Asset Management, CDM Defend Identity and Access Management, and CDM Defend Bounding 1, the Department relied on a "gap fill" (whereas operations change, capabilities are up-to-date) assessment that was initiated with DHS.

The Department's Information Security Continuous Monitoring (ISCM) strategy captured its inventory monitoring and includes hardware assets and high value assets. The Department reviewed and updated inventory at least annually, and sometimes quarterly. The Department maintained its inventory of hardware assets using a Configuration Management Plan template. The ISCM Strategy also addressed the responsibility for maintaining information technology assets and managing software.

The Department had a process to track its corrective action plans for security weaknesses, and it maintained and tracked these plans using the Cyber Security Assessment and Management tool. This included the centralized tracking of security weaknesses, prioritization of remediation efforts, maintenance, and independent validation of corrective action plans. The Cyber Security Assessment and Management tool provided the capability to automatically alert responsible parties (such as the system owner, Information System Security Officer, or Authorizing Official) about upcoming corrective action plan milestone due dates. The system owner and Information System Security Officer must monitor corrective action plan progress. The Department used an independent verification and validation process to ensure that corrective action plan milestones were monitored and tracked to completion.

However, the Department's practices in 11 of the 12 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 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. Finding 1 identifies the several areas needing improvement for this metric domain.

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

We found that for the Risk Management metric domain, the Department and FSA were at the Optimized level for 1 metric question, the Consistently Implemented level for 1 metric question, and the Defined level for 10 metric questions. We determined that the Department's and FSA's controls for the corrective action plan process needed improvement.

Department and FSA's Corrective Action Plan Remediation Process Needs Improvement

The Department and FSA did not provide effective oversight of their corrective action plan remediation process. Specifically, FSA did not remediate plans within the required timeframe because the appropriate official was not assigned for Plan of Action and Milestones (POA&M) remediation. We identified a total of 7,635 corrective action plans created from October 2009 through September 2019 attributable to FSA operational systems in FISMA reportable status in the Cyber Security Assessment and Management tool. For these 7,635 corrective action plans that were categorized by importance, 104 were classified as very high; 1,831 as high; 3,722 as medium; 1,948 as low; and 8 as very low. FSA established its POA&M standard operating procedure (which incorporates Federal guidance) requiring that POA&Ms must be resolved within a required timeframe

for each risk category—10 days for very high, 30 days for high, 90 days for medium, and 120 days for low and very low. However, we found that FSA did not resolve 1,034 POA&Ms in accordance with these timeframe guidelines of which 830 were not assigned to an Information System Security Officer to remediate as required.

To improve its oversight of the POA&M process, the Department developed its "Most Valuable POA&M" reports comprising very high and high risk POA&Ms to prioritize resources and address the most critical risks to the systems. These reports were also provided to FSA to assist in addressing the most critical risks to FSA systems. We obtained and reviewed the "Most Valuable POA&M "reports for the months of April 2019 through August 2019 and noted that FSA did not consistently meet timeline requirements. For example, POA&Ms categorized as very high in the April 2019 Most Valuable POA&M report and were therefore subject to the 10-day remediation, remained open until June 2019. One remaining open for 122 days.

The Department and FSA still relied on a manual and ad-hoc process for creating, managing, and monitoring POA&Ms in the Cyber Security Assessment and Management tool—the authoritative source for developing, managing, and maintaining the Department's inventory of information technology systems and system of record for FISMA reporting. The Cyber Security Assessment and Management tool was also the primary data feed for the Cybersecurity Framework Risk Scorecard, which will be the Department and FSA's primary tool for automating POA&Ms in the future. The Department and FSA were working to address issues with data accuracy and integrity within the Cyber Security Assessment and Management tool to ensure accurate POA&M tracking and reporting.

NIST Special Publication (SP) 800-53, Revision 4, 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 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.

Incomplete and inaccurate information, along with untimely remediation of corrective action plans could limit the Department's and FSA's abilities to assess system risk, evaluate funding requirements, and ensure adequate security of the systems is enforced.

Recommendations

We recommend that the Deputy Secretary and Chief Operating Officer require that OCIO and FSA—

1.1 Incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Risk Management program.

1.2 Ensure that POA&M remediation is performed within the required timeframe.

1.3 Ensure that all POA&Ms are assigned with the required appropriate remediation official.

Management Comments

The Department partially concurred with the Recommendation 1.1. It's the Department's understanding that there is a simply fundamental difference in opinion on the scoring methodology of this metric domain and cited its progress in managing POA&Ms for fiscal year 2019. It further expects to fully close the FY 2018 corrective action associated with this recommendation by September 30, 2021.

The Department partially concurred with Recommendation 1.2 and noted that it has made significant progress in resolving outdated POA&Ms. It states that it will continue this effort in FY 2020 and will develop a corrective action plan by December 31, 2019, to address this recommendation.

The Department also partially concurred with Recommendation 1.3. It stated that of the 830 POA&Ms identified by the OIG, 815 were created and closed in FSA's previous POA&M system of record and that during the migration of the POA&Ms to the Cyber Security Assessment and Management tool, the 'Assigned To' field did not populate for a number of POA&Ms for various reasons. Of the remaining 15 POA&Ms, 8 were created in error and procedurally closed prior to all fields being completed. To resolve this issue, FSA added the remediation official for the remaining 7 POA&Ms and conducted internal training to ensure this information is added to all future POA&Ms. Evidence was provided to OIG for this action for review.

OIG Comments

The Risk Management metric encompasses factors from each of the other metric domains. The metrics questions for the Risk Management metric domain and the evidence collected by OIG to answer those questions and to support metric domain scoring extend beyond FY 2019 POA&M remediation.

In April 2018, NIST issued its "Framework for Improving Critical Infrastructure Cybersecurity" to provide a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders. The five core

functions of the framework (Identify, Protect, Detect, Respond, and Recover) should be performed concurrently and continuously to establish an operational culture that addresses the dynamic cybersecurity risk. The Identify function comprises the Risk Management metric that encompasses factors from each of the other metric domains. Out of the eight metric domains, including Risk Management, six were assessed at the Defined Level.

In addition, we identified deficiencies that relate to risk management in other metric areas, such as (1) the Cyber Security Assessment and Management tool did not always produce consistently accurate results that would enable the Department to assess the risk; (2) for the 120 FISMA reportable systems identified in the Cyber Security Assessment and Management tool and found that only 17 of these systems had valid risk assessments completed; and (3) the Department has not fully implemented the DHS Continuous Diagnostics and Mitigation Program—in particular, Phase 1 and Phase 2 of the program—that includes hardware asset management, software asset management, configuration settings management, and vulnerability management. OIG will continue to monitor the Department's progress in closing out Recommendation 1.1.

For Recommendation 1.2, the Department indicated that it made significant progress in resolving outdated POA&Ms and committed to develop a corrective action plan by December 31, 2019 to address the recommendation. OIG 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 2020 FISMA audit fieldwork.

For recommendation 1.3, the Department indicated that the deficiency noted was due to the migration to the Cyber Security Assessment and Management tool, during which certain elements did not populate POA&Ms for various reasons. Subsequently, based on initial notification from OIG, the Department provided a description of actions it has taken, or intends to take, to address our finding and recommendations. If properly implemented, the actions would be responsive to our finding and recommendations.

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 and FSA's configuration management programs were consistent with the Defined level of the maturity model, which is considered not

effective. We identified areas where the Department and FSA made improvements to their configuration management program.

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 enables the management of system resources throughout the system life cycle.

The Department's primary configuration management policy was identified in the "Cybersecurity OCIO Policy 3-112." It also used the 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.

The Department established vulnerability and patch management processes to ensure that they were conducted in accordance with Federal guidance and mandates to minimize risk to Departmental information systems and networks.

The Department and FSA employed several scanning tools in their assessment of potential vulnerabilities on its networks. They also used outside services for scanning systems for vulnerabilities. We determined that the Department instituted mechanisms for tracking systems that are susceptible to security vulnerabilities. In addition, the Department established mechanisms for disseminating information on evolving cyber threats involving configuration management.

Both the Department and FSA maintained a configuration management database of all hardware and assets that enables them to define their security posture. We verified that the Department and FSA were tracking connection security of their external facing websites.

The Department established Information Technology Security Baseline Configuration Guidance that provides a uniform approach for installation, configuration, and maintenance of secure information technology system baseline configurations. The Department followed the OMB-mandated Federal Desktop Core Configuration.

However, its practices in all 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 needed to ensure that all systems required to transverse through a trusted or secure internet connection are configured accordingly, and all

obsolete systems are retired and replaced by a new solution. Finding 2 identifies several areas needing improvement for this metric domain.

Finding 2. The Department and FSA's Configuration Management Programs Need Improvement

We found that for the Configuration Management metric domain, the Department and FSA were at the Defined level for six metric questions and the Consistently Implemented level for two metric questions. We determined the Department and FSA's controls needed improvement for consistently using of secure connections; using appropriate application connection protocols; relying on vendor-supported operating systems, databases, and applications in its production environment; using a default username and password to access its voice over internet protocol solution; adequately protecting personally identifiable information; improving controls over web applications and servers; and consistently performing system patching.

Department Did Not Consistently Ensure the Use of Secure Connections

The Department did not consistently ensure that websites were configured to use a trusted internet connection or managed trusted internet protocol services. This occurred because the Department had not fully implemented these connections or services. We identified 84 systems that were required to use trusted internet connections as part of their processes. We found that only 51 (or 61 percent) of the systems were not configured to use a trusted internet connection or managed trusted internet protocol services solution as required by DHS and OMB requirements. The Department must ensure that systems are routed through a secure connection to safeguard student information and avoid a risk of compromise.

In addition, we found that the Department did not enable the use of an encryption protocol on 9 of the 602 websites in its inventory to protect users and their information being submitted via web portals. However, we noted that the Department made significant progress in this area since the FY 2017 FISMA audit. In FY 2017, we reported that the Department did not enable an encryption protocol on 151 out of 478 websites. In FY 2018, we found this number decreased with only 6 out of 653 websites not enabling the use of an encryption protocol. According to OCIO, the Department continues to address this vulnerability with the goal to become compliant with DHS Binding Operational Directive 18-01, "Enhance Email and Web Security." OMB M-15-13, "Policy to Require Secure Connections Across Federal Websites and Web Services," requires that all publicly accessible Federal websites and web services provide service only through a secure connection. Further, agencies were required to make all existing websites and services accessible through a secure connection (HTTPS-only, with HSTS)

by December 31, 2016.[8] Through the use of secure connections, the Department can ensure that data transmissions are protected and decrease the risk of compromise.

Department and FSA Did Not Use Appropriate Application Connection Protocols

We found that the Department and FSA continue to use outdated secure connection protocols. Specifically, we identified that 5 out of 602 authorized connections used Transport Layer Security 1.0. Until the Department and FSA ensure that all secure connections adhere to the required protocols, users could still expose systems to vulnerabilities and exploits, including man-in-the-middle attacks that could jeopardize Department resources.[9] We reported a similar condition in our FY 2016, 2017, and 2018 FISMA audits. NIST SP 800-52, "Guidelines for the Selection, Configuration and Use of Transport Layer Security Implementations," states that Transport Layer Security version 1.1 is required, at a minimum, to mitigate various attacks on version 1.0 of the Transport Layer Security protocol. Support for Transport Layer Security version 1.2 is strongly recommended and agencies are required to develop migration plans to support Transport Layer Security 1.2 by January 1, 2015.[10]

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

We found that 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 1,099 systems listed, 47 were identified as running with obsolete operating systems. The Department relied on Risk Acceptance Forms to continue using unsupported operating systems, databases, and applications. Continued use will make these information technology solutions vulnerable to intentional and unintentional compromise. FSA stated that the migration plan to move systems to a

---

[8] Hypertext Transfer Protocol (or HTTP) is the foundation of data communication for the World Wide Web. HTTPS is the secure version of HTTP. HTTPS Strict Transport Security (or HSTS) allows web servers to declare that web browsers should only interact with it using secure HTTPS connections.

[9] A man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who are directly communicating with each other.

[10] NIST 800-52 Revision.2 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.

new data center environment will help retire and discontinue the use of the unsupported systems. Relying on unsupported operating systems, databases, and applications, could lead to data leakage and exposure of personally identifiable information 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. We reported similar conditions in our 2017 and FY 2018 FISMA audits.

Default Username and Password Used on Polycom Voice Over Internet Protocol Solution

The Department used a web portal for managing a Polycom Voice Over Internet Protocol solution that allowed users to authenticate using a default username and password. Most concerning, we were able to determine the default username and password by using a public online search. Users authenticating through the web portal have administrative privileges to the Voice Over Internet Protocol solution that would allow an unauthorized user to make changes to the solutions configuration settings, such as issuing or changing user passwords that would lock system owners out of the solution. It is imperative that the Department ensure that all username and passwords are changed before placing that solution on the network.

When we identified the vulnerability for this solution, we notified the Office of the Chief Information Officer. We performed follow-up testing in July 2019 and confirmed that the Department had remediated the vulnerability.

Personally Identifiable Information Not Consistently Protected

FSA did not ensure that all websites mask personally identifiable information—primarily Social Security numbers—that users enter on the sites. During our review of 602 websites, we identified one externally hosted website using Social Security numbers that lacked adequate protection. Two of the externally hosted websites were not configured to mask sensitive personally identifiable information (including Social Security numbers and birth dates) and instead displayed the information in plain text as it was entered. One of these two sites used a Social Security number as a primary identifier. We found FSA did not consistently implement appropriate controls to safeguard the security and confidentiality of records and enforce the protection of personally identifiable information. OMB M-06-15 – states each agency is required to establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records. In addition, OMB M-07-16 states each Agency must participate in government-wide efforts to explore alternatives to agency use of Social Security numbers as a personal identifier for both Federal employees and in Federal programs. We have reported a similar condition relating to using Social Security

numbers as a primary identifier in our FY 2014, 2017, and 2018 FISMA audits.

FSA's Controls over Web Applications and Servers Need Improvement

FSA web-applications vulnerabilities increase the risk of unauthorized access to critical security architecture. We assessed web application security for eight of the nine systems judgmentally selected for testing.[11] We found that FSA needed to improve controls related to implementing and managing its technical security architectures supporting applications and infrastructure to restrict unauthorized access to information resources and protect it against potential application compromise. We also found that although some key controls were effectively implemented (such as data validation, secure coding, and web security), we identified key controls that were not in place to restrict unauthorized access to the security architecture. For example, we identified instances of (1) Structured Query Language injection execution vulnerabilities, (2) cross-site scripting, (3) cross-site forgery, (4) the ability to inject and execute hypertext markup language code, (5) displaying Social Security numbers in clear text, (6) unrestricted file upload, (7) no client side input validation, (8) files not fully deleted (can be recovered if not overwritten), (9) backup/restore mechanism not disengaged (sensitive information can be stored and accessed), and (10) ability to modify payment information. We determined FSA 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 its resources. We reported similar conditions in our FY 2017 and FY 2018 FISMA audits.

FSA System Patching Was Not Consistently Performed

We found that FSA did not consistently apply software patches and security updates to its systems and information technology solutions. We identified instances where critical patch updates and security updates were not applied, as well as information technology solutions that were vulnerable to zero-day exploits. A zero-day exploit is a hacking attack that leverages a zero-day vulnerability to compromise a system or device. Failure to patch systems would allow a malicious user to gain access to a system and user accounts, leading to identity theft or fraud. Most notably, some of the systems identified with issues were obsolete and therefore, the patches are no longer available from the vendor. In addition, patches were not applied to systems on a regularly scheduled basis. We reported similar conditions in our FY 2017 and FY18 FISMA audits.

[11] See the "Scope, and Methodology" section of this report for a complete list of systems we tested.

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) minimization of personally identifiable information, (3) unsupported system components, (4) transmission confidentiality and integrity; and (5) changing default content of authenticators.[12]

NIST SP 800-46, Revision 2, "Guide to Enterprise Telework and Remote Access, Bring Your Own Device (BYOD) Security," states that organizations should consider the use of network access control solutions that verify the security posture of a client before allowing these on an internal network.

Recommendations

We recommend that the Deputy Secretary and Chief Operating Officer require that OCIO and FSA—

2.1 Incorporate additional measures to, at a minimum; achieve Level 3 Consistently Implemented status of the Configuration Management program.

2.2 Migrate to Transport Layer Security 1.2 or higher as the only connection for all Department connections.

2.3 Review new solutions to ensure that the default username and password has been changed.

We recommend that the Deputy Secretary require OCIO to—

2.4 Ensure that 51 websites are routed through a trusted internet connection or managed trusted internet protocol service.

2.5 Ensure that all existing websites and services are accessible through a secure connection as required by OMB M-15-13.

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

We recommend that the Chief Operating Officer require FSA to—

2.6 Discontinue the use of unsupported operating systems, databases, and applications.

2.7 Ensure that all websites and portals hosting personally identifiable information are configured not to display clear text.

2.8 Eliminate the use of Social Security numbers as an authentication element when logging into FSA websites by requiring the user to create a unique identifier for account authentication. (Repeat Recommendation)

2.9 Immediately correct or mitigate the vulnerabilities identified during the security assessment.

Management Comments

The Department concurred with Recommendation 2.1 and expects to close the FY 2018 corrective action associated with the recommendation by September 30, 2021. For Recommendations 2.2, 2.4, and 2.5, the Department concurred, noting that similar recommendations were issued in FY 2018 and that it expects the corrective actions to be completed by February 28, 2020 (Recommendations 2.2 and 2.5) and October 30, 2020 (Recommendation 2.4). For Recommendation 2.3, the Department concurred with the recommendation and state that it requested immediate remediation by the service provider and issued a contractual letter of concern, with the evidence provided to the OIG. For Recommendations 2.6 and 2.9, the Department will develop a corrective action plan by December 31, 2019, to address the recommendations.

The Department did not concur with Recommendations 2.7 and 2.8. For both recommendations, the Department stated that it accepted the risk due to business requirements. It further stated that FSA continues to research viable alternative approaches and will move to fix this deficiency once a suitable option is found. The Department further stated that in accordance with its risk management practices, it will periodically review the business requirements and conditions for risk acceptance.

OIG Response

OIG will continue to monitor the Department's progress in closing out Recommendations 2.1 and 2.4. For Recommendations 2.2 and 2.5, OIG will validate the corrective actions taken during our FY 2020 FISMA fieldwork. For Recommendations 2.6 and 2.9, OIG will review the corrective action plans and assess whether the actions will address the finding and recommendations during our FY 2020 FISMA audit fieldwork.

For Recommendation 2.3, OIG agrees that the vulnerability was remediated for the Voice Over Internet Protocol; however, the recommendation asks that the Department

establish a process to ensure that default usernames and passwords are not being used for other solutions. Therefore, the Department needs to establish a corrective action plan to ensure that this does not occur for other solutions used by the Department.

For Recommendations 2.7 and 2.8, OIG considered the Department's response and did not revise the finding or recommendations. For both recommendations, OIG agrees with the Department's ongoing efforts to research alternative approaches and find a suitable solution to address this deficiency. However, OIG does not agree with the Department's decision to accept the risk due to business requirements because the Department did not inform the OIG of the mitigating controls in place and operating to support that decision. Therefore, users are entering personally identifiable information that is not being masked or obfuscated, making the entered data vulnerable to several attacks including screen-captures, shoulder-surfing, and key logging attacks. OMB Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," instructs agencies to reduce the use of social security number by eliminating unnecessary use and explore alternatives. NIST SP 800-53, Revision 4, further requires that organizations locate and remove/redact specified personally identifiable information and/or use anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure. Both similar conditions and recommendations were reported to FSA in the FY 2017 and FY 2018 FISMA audits. In both audits, FSA concurred with the finding and recommendation. Although FSA is accepting the risk, it is not fully complying with OMB and NIST guidance and needs to identify and implement an alternative solution to ensure that appropriate controls are in place to protect individuals from unnecessary exposure.

METRIC DOMAIN 3—IDENTITY AND ACCESS MANAGEMENT

We determined that the Department's and FSA's identity and access management programs were consistent with the Defined level of the maturity model, which is considered not effective. We identified areas where the Department and FSA made improvements to its identity and access program.

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.

The Department updated the OM: 5-101, "Personnel Security Screening Requirements for Contractor Employees." In addition, ICAM requirements were deployed during PIVOT Phase 1, such as, Dell Security End Point Protection. Furthermore, in December 2018, FSA issued its "Managing Privileged User Accounts" standard operating procedure to address the management of privileged account security.

We found that the Department established identity and access management policies, procedures, and guidance that comply with NIST and OMB standards. In June 2018, the Department established the ICAM program charter and continued to rely on the charter that established program authority to improve coordination, management, and oversight for the realization of the Federal ICAM program within the Department. The program also helped increase security, enforce compliance with laws and regulations, improve operability, enhance customer service, eliminate redundancy, and increase protection of personally identifiable information.

OCIO established the "Identity, Credential, and Access Management Enterprise Roadmap, Version 2.0," dated August 2017. The strategy for Enterprise ICAM was intended to address the gap between technology concept, maturation, and adoption; drive the need for interoperability of an enterprise ICAM solution; allow for the evolution of ICAM capabilities to accommodate future needs of the Department's overall information assurance strategy and the defined ICAM business objectives; and ensure solutions are secure, resilient, cost effective, and easy to use. OCIO also developed a Departmental ICAM Implementation Plan, version 3, dated August 2018 that provides a high-level description of the processes and tasks needed to implement a comprehensive, enterprise-wide ICAM solution. The Department documented and defined ICAM stakeholder roles and responsibilities within the ICAM Program Charter and Implementation Plan and Enterprise Roadmap, which were disseminated to stakeholders through the Department's intranet.

In December 2018, FSA issued its "Managing Privileged User Accounts" standard operating procedure that addresses the management of users with privileged and non-privileged access to FSA internally and externally hosted systems. Although not fully implemented, the standard operating procedure outlines a process for tracking and reporting FSA contractors with access and removal of access to internally and externally hosted systems.

However, its practices in all nine metric questions still do not meet the Managed and Measurable level of maturity or an effective level of security. The Department and FSA 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 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 and FSA's Identity and Access Management Program Needs Improvement

We found that for the Identity and Access Management metric domain, the Department and FSA were at the Defined level for eight metric questions, and Ad Hoc level for one metric question. We determined that the Department and FSA's controls needed improvement for implementing the ICAM strategy, managing privileged user accounts, fully implementing two-factor authentication, fully configuring the network access control solution, removing access of terminated users to the Department's network, ensuring virtual private network connections disconnect after 30 minutes of inactivity, improving controls over database management, configuring websites to display warning banners, consistently documenting and maintaining access agreements before granting access to systems, and consistently documenting position risk descriptions for background investigations.

Department's ICAM Strategy Not Fully Implemented

During our FY 2017 FISMA audit, we found that the Department was in the process of creating its ICAM structure and expected to have full implementation of ICAM by the end of FY 2018. However, during the FY 2018 FISMA audit, we found that because of a contract dispute, a delay occurred in the awarding of the PIVOT contracts that would have helped ensure full implementation of an Enterprise ICAM solution. The Enterprise ICAM solution is scheduled for completion by December 31, 2020. During the FY 2019 FISMA audit, we found that all PIVOT contracts were awarded, and transition activities were completed on July 31, 2019. Without full implementation of the ICAM strategy, the Department cannot ensure its full accountability of its access management systems, especially those hosted externally. The Department's FISMA inventory consisted of 121 reportable systems of which 85 were hosted at various external contractor sites, including Federal Risk and Authorization Management Program (FedRAMP) cloud service provider locations. These also include the Department's High Value Asset systems, which were applications and systems that directly support mission essential functions.

FSA Did Not Fully Implement a Process to Manage Privileged Accounts

We found that FSA did not fully implement a process for identifying, managing, or tracking activity of privileged accounts. We requested evidence of FSA's privileged user account review for the second quarter of 2019 (covering January through March 2019), that included evidence of audit log analysis—which is required by FSA's standard operating procedure, "Managing Privileged User Accounts." However, we were not provided with evidence of privileged user account review and audit log analysis so that

we could validate that this process occurred. As part of its 2018 corrective action plan, the Department planned to implement a process to manage and track activity of privileged users by January 31, 2019. However, we confirmed the planned implementation date of this process was extended to September 30, 2019. Without an accurate accounting, tracking and reviewing of privileged users accessing Departmental systems and its resources, as well as not reviewing privileged user activities, the Department has no assurance that privileged user activity did not result in the compromise of its systems and data. We reported this condition during our FY 2017 and FY 2018 FISMA audits.

FSA Did Not Fully Implement Two-Factor Authentication

We found that FSA did not consistently enforce the use of two-factor authentication. For 602 FSA websites identified, we used the Uniform Resource Locator Profiler tool to assess the security posture and determine whether the websites complied with Federal guidance. Our testing found that of the 602 websites, 19 were not configured to use two-factor authentication. Failure to implement two-factor authentication will allow a user with a username and password to remotely connect and access network resources. This unrestricted access could lead to leakage and data exposure. On August 27, 2004, the President signed Homeland Security Presidential Directive-12 "Policy for a Common Identification Standard for Federal Employees and Contractors" which requires the development and implementation of a mandatory, government-wide standard for secure and reliable forms of identification for Federal employees and contractors. We reported a similar condition in our FY 2011 through FY 2018 FISMA audits.

Network Access Control Solution Not Fully Configured

Since FY 2011, we have reported that the Department did not enable its Network Access Control Solution to restrict the use of unapproved non-Government Furnished Equipment on its network. In our FY 2018 FISMA audit testing, we found that the Department had enabled the ability of its Network Access Control Solution to restrict non-Government Furnished Equipment from connecting to the network. However, during our FY 2019 FISMA testing, we found that the Department's Network Access Control Solution allowed unapproved non-Government Furnished Equipment to connect to the network and maintain that connection once user access was granted. The Department did not provide a determination about why OIG was able to connect to the network with an unapproved non-Government Furnished Equipment. By allowing an unapproved device to authenticate to the Department's network, the Department may enable a malicious actor to launch an attack or gain intermittent access to internal network resources that could lead to data leakage or data exposure.

Terminated Users with Access to Departmental and FSA Systems

During our FY 2018 FISMA audit, we found the Department and FSA did not remove user access to the network for people who were terminated from employment. As part of its corrective action plan, the Department planned to implement its process to disable account for terminated employees by September 30, 2019. This completion date was outside our audit period, so at the time of the audit, the Department had not yet completed this corrective action. Terminated employees whose user accounts remained active with access to critical Department or FSA systems and resources increase the risk of unauthorized access by malicious users and compromise Departmental information resources. Furthermore, the lack of oversight for ensuring terminated user access decreases the Department's visibility into its network activity and thus the tracking inactive user accounts accessing critical Department and FSA systems and resources.

Virtual Private Network Connection Does Not Disconnect After 30 Minutes of Inactivity

During our testing of all uniform resource locator website inventory provided by the Department and FSA, we found that the new virtual private network connection (Global Protect Virtual Private Network) was not configured to disconnect a user after 30 minutes of inactivity. During our testing process, we used a personal identity verification card to authenticate the account and connect to the virtual private network. After 30 minutes of inactivity, the user was not disconnected from the network. During two separate tests, the connection remained online for over 2 hours without being disconnected from the network. We requested logs from FSA to validate the virtual private network connections, duration time, and time of disconnect. However, FSA did not provide the logs during our fieldwork. We determined FSA did not enforce configuration management security controls required by NIST 800-53, Revision 4, regarding the testing of configuration changes. Without properly testing the virtual private network time-out feature functionality, there is a risk that users could expose the Department's networks to unauthorized users and compromise the confidentiality, integrity, and availability of information systems increases. We reported a similar condition in our FY 2011, FY 2012, FY 2015 and FY2018 FISMA audit reports.

FSA's Controls over Database Management Need Improvement

We performed assessments that identified vulnerabilities, configuration errors, and access issues for databases included in three of nine systems in our judgmentally selected sample—the Enterprise Data Warehouse Analytics, Nelnet Servicing, and the Debt Management Collection System. Scans of databases associated with these systems identified 44 high vulnerabilities, 94 medium vulnerabilities, and 50 low vulnerabilities. FSA had not consistently implemented the necessary controls to ensure that its databases were protected. We shared the vulnerabilities with FSA for remediation. By allowing these vulnerabilities to exist, the Department increases the risk that

unauthorized individuals can access or alter the data. We reported similar conditions in our FY 2017 and 2018 FISMA audits.

FSA Did Not Configure All Websites to Display Warning Banners

We found that 60 of 602 FSA websites were either missing warning banners or displaying banners that did not use standard Federal regulation language. We used the Uniform Resource Locator Profiler Tool to assess the security posture of the 602 websites and determine whether they complied with Federal guidance. The Department communicated to its stakeholders, including FSA, that banners and acceptable text are required to be in place by October 1, 2018. In the Department's corrective action plan for the FY 2018 FISMA audit the Department planned to finish configuring all websites to display warning banners by October 31, 2019. Department policies and NIST guidance mandate a warning banner alerts users that they are accessing a government website. At a minimum, warning banners should state that users should not expect any privacy when connecting to an information technology asset owned or operated on behalf of the Department. We reported a similar condition in our FY 2017 and FY 2018 FISMA audits.

Access Agreements Were Not Properly Documented and Maintained

The Department and FSA did not consistently document access agreements for people before granting access to their network and systems. We judgmentally selected 15 new users (10 from Departmental offices and 5 from FSA systems tested during the audit). We found that for 10 users (8 Department and 2 FSA), access agreement forms were not documented and maintained. The Department and FSA did not provide documentation to verify that access agreements existed for these users. As a result, the Department and FSA did not have assurance that new users acknowledged the terms of access agreements by signing the documents and that they were aware of existing terms of access. This increases the risk that users may unintentionally disclose sensitive information or act in a manner contrary to Department policies, procedures and guidelines.

Position Risk Designation Records Not Properly Documented for Background Investigations

Position risk designations were not consistently documented for background investigations. We judgmentally sampled 40 users (28 privileged and 12 nonprivileged), all of which were contractor employees, and requested evidence that a risk designation was performed and documented for each user. The Department and FSA were unable to provide documented evidence that a risk designation was prepared for any of the 40 users. The "Contractor Employee Personnel Security Screenings Handbook," February 28, 2019, states that the principal office will analyze and determine the risk level designations and the corresponding level of background investigations required in

their contracts. The position risk/sensitivity level for all contractor employees must be determined and documented before contract acquisition. The Department relies on system owners to complete position risk designations for new users. We found the Department and FSA did not consistently oversee of documenting access agreements for users accessing agency systems. Allowing users without proper clearance to access these systems and resources increases the risk of unauthorized access to malicious users and could compromise Departmental information 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) access control, identification and authentication; (2) account management; (3) system use notification; (4) remote access; (5) rules of behavior; (6) access agreements; (7) information system monitoring; and (8) removal of temporary and emergency accounts.

Recommendations

We recommend that the Deputy Secretary and Chief Operating Officer require OCIO and FSA to—

3.1 Incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Identity and Access Management program.

3.2 Ensure that terminated users' network access is removed timely.

3.3 Ensure that access agreements for users accessing Department and FSA systems are documented and maintained. (Repeat Recommendation)

3.4 Consistently document position risk designations for background investigations.

We recommend that the Deputy Secretary require OCIO to—

3.5 Fully implement the Department's ICAM strategy to ensure that the Department meets full Federal government implementation of ICAM. (Repeat Recommendation)

3.6 Ensure that the network access control solution is fully implemented to ensure identification and authentication of devices connected to the network.

3.7 Validate the inactivity settings to ensure sessions time out after 30 minutes of inactivity.

We recommend that the Chief Operating Officer require FSA to—

3.8 Fully implement the process for identifying, managing, and tracking activity of privileged user accounts.

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

3.10 Create corrective action plans to remedy database vulnerabilities for all database vulnerabilities identified.

3.11 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.

Management Comments

The Department concurred with Recommendation 3.1 and expects to close the FY 2018 corrective action associated with the recommendation by September 30, 2021. For Recommendations 3.2 and 3.8, the Department concurred citing that similar recommendations were issued in FY 2018 and the Department updated its account management procedures to address the recommendations. For Recommendations 3.3, 3.4, 3.7, 3.9, and 3.10 the Department stated that it will develop a corrective action plans by December 31, 2019, to address the recommendations. The Department concurred with Recommendations 3.5, 3.6, and 3.11 and expects to close the FY 2018 corrective actions associated with the recommendations by December 31, 2020 (Recommendation 3.5), and October 31, 2019 (Recommendations 3.6 and 3.11).

OIG Response

OIG will continue to monitor the Department's progress in closing out Recommendations 3.1 and 3.5. For Recommendations 3.2 and 3.8, OIG will validate the corrective actions during our FY 2020 FISMA fieldwork. For Recommendations 3.3, 3.4, 3.6, 3.7, 3.9, 3.10, and 3.11, OIG will review the corrective action plans to determine if the actions will address the finding and recommendations and if so, will validate the corrective actions taken during our FY 2020 FISMA audit fieldwork.

METRIC DOMAIN 4—DATA PROTECTION AND PRIVACY

We determined that the Department's and FSA's data protection and privacy programs were consistent with the Defined level of the maturity model, which is considered not effective. We identified areas where the Department and FSA made improvements to its data protection and privacy program. We identified areas where the Department and FSA made improvements to its data protection and privacy program.

Personally identifiable information 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 personally identifiable information 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 fundamental responsibility to protect the privacy of individuals' personally identifiable information that they collect, use, maintain, share, and dispose of by programs and information systems.

The Department established policies and procedures for data protection and privacy. For instance, the directive on "Privacy: Section 208 of the E-Government Act of 2002 Policy and Compliance," September 6, 2016, outlines the roles and responsibilities for the effective implementation of the organization's privacy program for key officials, offices, and contractors.

The Department established a Privacy Program Plan that defines its process for protecting the privacy rights of all individuals whose information it collects. Also, the OCIO and Privacy Office developed a Data Breach Response Plan that incorporates requirements identified in OMB Memorandum 17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information." The plan defined the roles and responsibilities for key positions throughout the Department.

The Department established data protection security controls that include least privilege, data loss prevention, and use of encryption tools to prevent data exfiltration and enhance network defense. The Department also established a data loss prevention system that is an automated tool to monitor outgoing unencrypted employee email (including attachments) and web traffic to identify sensitive information. It is designed to detect email containing unencrypted sensitive information and prevent it from leaving the Department's boundary.

As part of the Department's data protection and privacy process, it established the use of Privacy Impact Assessments, System of Records Notices, and Privacy Threshold Analyses. A Privacy Impact Assessment is an analysis of how information in identifiable form is collected, maintained, stored, and disseminated. The assessment also examines and evaluates the privacy risks and the protections and processes for handling information to mitigate those privacy risks. Privacy Impact Assessments are reviewed every 2 years to determine whether any significant changes have occurred that create new privacy risks. A System of Records Notice informs the public about what kinds of protected personal information Federal agencies maintain, limits the use and disclosure

of the information to those compatible with the law permitting its collection, and describes how someone can request access to their information or seek redress. A Privacy Threshold Analysis is a short form used to determine whether a system contains personally identifiable information, whether a Privacy Impact Assessment or System of Records Notice is required, and whether any other privacy requirements apply to the information system.

For the nine systems we reviewed this year, we determined whether each system had documented a Privacy Impact Assessment, System of Records Notice, and Privacy Threshold Analysis. Overall, we found that the Department had documented System of Records Notices and Privacy Threshold Analyses for the systems we selected. However, we found that Privacy Impact Assessments were not maintained for seven of the nine systems, as discussed in the finding section below.

Despite the improvements we identified, Department and FSA practices in all five metric questions still do not meet the Managed and Measurable level of maturity or an effective level of security. The Department and FSA would need to achieve a Managed and Measurable level on at least three of the five metric questions to achieve and effective Data Protection and Privacy metric domain. For example, the Department and FSA would need to ensure the consistent and timely reviews of Privacy Impact Assessments. Finding 4 identifies several areas needing improvement for this metric domain.

Finding 4. The Department's and FSA's Data Protection and Privacy Program Needs Improvement

We found that for the Data Protection and Privacy metric domain, the Department and FSA were at the Defined level for all five metric questions. We determined that the Department and FSA's controls for the consistent and timely reviews of Privacy Impact Assessments needed improvement. In addition, we identified other areas affecting data protection and privacy, which we address under other metric domains in this report.

Department Did Not Consistently Perform Timely Reviews of Privacy Impact Assessments

We found that the Department did not consistently perform timely reviews of system Privacy Impact Assessments. The Department's Privacy Program Plan requires that Privacy Impact Assessments be reviewed every 2 years; however, the Department did not timely review Privacy Impact Assessments for seven of the nine systems we judgmentally selected for review. The Department stated that an effort was currently underway with a specific resource dedicated to identifying and updating Privacy Impact Assessments; however, this effort was still in progress. Without a consistently implemented Data Protection and Privacy program, the Department will not be able to

determine whether any significant changes to the collection, maintenance, storage, and dissemination of privacy information on Departmental systems has occurred—potentially creating new privacy risks to said information.

Other Report Findings Impacting Data Protection and Privacy

In the Protect security function, under the section for the Configuration Management metric domain, we report on FSA websites that were not protecting personally identifiable information by allowing Social Security numbers to be displayed unmasked and used as identifiers. Also, in the Respond security function, under the Incident Response metric domain, we found weaknesses in the Department's data loss prevention capabilities that allowed personally identifiable information to be unblocked during email transmission.

OMB Circular A-130, "Managing Information as a Strategic Resource," July 28, 2016, requires Federal agencies to develop and maintain a privacy program plan that provides an overview of the agency's privacy program. This includes a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the senior agency official for privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks, and any other information determined necessary by the agency's privacy program. Also, the Department's Privacy Program Plan states that Privacy Impact Assessments are reviewed every 2 years to determine whether any significant changes have occurred that create new privacy risks.

Recommendations

We recommend that the Deputy Secretary and the Chief Operating Officer require OCIO and FSA to—

4.1 Incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Data Protection and Privacy program.

We recommend that the Deputy Secretary require OCIO to—

4.2 Ensure that Privacy Impact Assessments are reviewed every 2 years.

Management Comments

The Department concurred with Recommendation 4.1 and expects to close the FY 2018 corrective action associated with the recommendation by September 30, 2021. For Recommendation 4.2, the Department concurred and expects to close the FY 2018 corrective action associated with this recommendation by November 28, 2019.

OIG Response

OIG will continue to monitor the Department's progress in closing out Recommendation 4.1, and if 4.2 is closed by the expected date, OIG will validate the corrective actions taken during our FY 2020 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. We identified areas where the Department and FSA made improvements to its security training program.

Security awareness training is a formal process for educating employees and contractors about information technology 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 information technology security policy, procedures, and practices; and have adequate knowledge of the various management, operational, and technical controls required to protect the information technology resources for which they are responsible.

The Department's Handbook, "Information Assurance Cybersecurity Policy," mandates that all personnel and supporting contractors receive training both before accessing its information systems and at least annually by the designated due date(s). It also incorporates the Federal Cybersecurity Workforce Assessment Act of 2015 to define and establish specialized training requirements. Additionally, the Department's Cybersecurity Awareness and Training Program Guidance," which incorporates NIST guidance, defines and establishes its Cybersecurity Awareness and Training Program. The Department communicates its policies through information technology points of contact meetings, ad hoc meetings with partners, Department-wide emails, town hall meetings, and the Department's intranet.

The Department established a Cybersecurity Awareness and Training Program to help reduce risk to its systems and information assets by changing human behavior and informing its personnel about security risks associated with their activities and responsibilities. The Department's "Cybersecurity Awareness and Training Program Guidance," January 25, 2018, establishes a security training program that focuses on informing personnel of their responsibilities in complying with Departmental policies and procedures designed to reduce risks and support the continuous growth and development of the cybersecurity workforce.

The Department used the annual Cybersecurity and Privacy Awareness training, covering employees and contractors, as one method of assessing whether staff has the

knowledge, skills, and abilities to perform their assigned work. It offered three Cybersecurity and Privacy Awareness trainings each year to assess the skills and knowledge of employees and contractors. New employees and contractors were also required to participate in the Cybersecurity and Privacy Awareness training program before accessing the Department's network. The Department tracked employees and contractors who failed to take the Cybersecurity and Privacy Awareness trainings. In addition, the Department defined the process to assess personnel with significant security responsibilities to ensure that they received appropriate training and education to develop and maintain a cyber security workforce capable of actively reducing and managing risk to its assets.

In 2017, the Department established a phishing program that included three simulated phishing exercises throughout each fiscal year. This phishing program allowed the Department to send simulated phishing emails to its employees and contractors and evaluate the effectiveness of its Cybersecurity and Privacy Awareness training. The results of the phishing exercises were then summarized to better assist the Department in evaluating the number of users who clicked on each simulated phishing email by each program office.

In April 2019, the OCIO issued a revised memorandum, "Requirements for Role-Based Training of Personnel with Significant Security Responsibilities," that requires the Department to identify personnel with significant security responsibilities and provide security training commensurate with their responsibilities. The Department also developed the Cybersecurity Awareness and Training Program Guidance, which establishes the requirements needed for system users to receive specialized training based on their roles and responsibilities. It also established a process to identify all positions within the agency that require the performance of information technology cybersecurity and assigned the corresponding Office of Personnel Management Cybersecurity Data Standard Codes to each of these positions after conducting an assessment of the knowledge, skills, and abilities of its cybersecurity personnel to determine the appropriate content of security training.

Despite these action, 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 skilled personnel have been hired or existing staff are continuously trained to have the appropriate skills and knowledge to protect the Department's assets and information. Finally, the Department would need to develop and implement the appropriate metrics to measure the effectiveness of the organization's training program in closing identified skill gaps. Finding 5 identifies several areas needing improvement for this metric domain.

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

We found that for the Security Training metric domain, the Department and FSA were at the Defined level for four metric questions and Consistently Implemented for two metric questions. We determined that the Department and FSA needed to improve their controls over the processes for ensuring staff completed role-based training and new employees completed training before they received network access.

Role-Based Training Not Consistently Completed

In March 2018, the Chief Information Security Officer issued a memorandum, "Requirements for Role-Based Training of Personnel with Significant Security Responsibilities," that describes the requirements for employees with significant security responsibilities to take role-based training. However, we found the Department did not fully implement a process for ensuring that staff completed role-based training. Specifically, for 28 judgmentally selected FSA contractors with privileged access, we found that 12 did not complete specialized security training (role-based training), as required by Federal regulations and Departmental policies. The Department and FSA relied on contracting officer's representatives, who used a manual process, to track the completion of contractor role-based training requirements. The Department did not have a mechanism to verify the manual process is accurately tracking role-based training requirements. Without an effective process to ensure that all users with significant security responsibilities (such as privileged users) have completed their role-based training, a user may not possess the adequate knowledge and skills necessary to assist them in carrying out their job function in a secure manner. Furthermore, ensuring that users with significant security responsibilities complete role-based training enhances an organization's security posture through a trained workforce and increases the individual's readiness to respond to security incidents.

New Users Were Granted Network Access Before Completing 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 590 new users that started employment with the Department from October 2018 through February 2019. We judgmentally selected 10 new users (4 Department employees and 6 contractors) and found that network accounts for five (1 Department employee and 4 contractors) were created before the new users took 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 they fulfilled 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 and FY 2018 FISMA audits.

NIST SP 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," requires organizations to provide role-based security training to personnel with assigned security roles and responsibilities. In addition, the Department's memorandum "Requirements for Role-Based Training of Personnel with Significant Security Responsibilities," April 17, 2019, requires all employees and contractors with significant security responsibilities to complete role-based training annually. FSA's "Annual Security Training Standard Operating Procedure," Version 2.3, July 23, 2018, states that employees and contractors who have significant or substantial security roles are required to take role-based training commensurate to their role.

Recommendations

We recommend that the Deputy Secretary require OCIO to—

5.1 Incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Security Training program.

5.2 Ensure that all new users complete the mandatory training requirements before they receive access to Departmental systems.

We recommend that the Deputy Secretary and the Chief Operating Officer require OCIO and FSA to—

5.3 Ensure that the process for ensuring completion of role-based training is fully implemented.

Management Comments

The Department concurred with Recommendation 5.1 and expects to close the FY 2018 corrective action associated with the recommendation by September 30, 2021. The Department also concurred with Recommendation 5.2 and cited a similar recommendation issued during the FY 2018 FISMA audit stating that it updated its account creation procedures to address the recommendation and provide OIG evidence of the action. For Recommendation 5.3 and will develop a corrective action plan by December 31, 2019, to address the recommendation.

OIG Comments

OIG will continue to monitor the Department's progress in closing out Recommendation 5.1. For Recommendation 5.2, although the Department stated that it updated its

account creation procedures, OIG still identified instances where the procedures were not consistently followed. For Recommendation 5.3, OIG 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 2020 FISMA audit fieldwork.

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 and FSA continued to develop and strengthen their ISCM program. However, we noted that improvements were needed in the Department and FSA's ability to (1) fully implement the Department's ISCM strategy, (2) fully implement the CDM program, and (3) ensure Cyber Security Assessment and Management tool data are accurately reflected in Cybersecurity Framework Risk Scorecard.

METRIC DOMAIN 6—INFORMATION SECURITY CONTINUOUS MONITORING

We determined that the Department's and FSA's ISCM programs were consistent with the Defined level of the maturity model, which is considered not effective. We identified areas where the Department and FSA 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.

The Department was participating in DHS's CDM program. The Department had partially implemented its DHS CDM capabilities for Phase 1: Hardware Asset Management, Software Asset Management, Configuration Settings Management, and Vulnerability Management. The Department was able to fully integrate its Agency CDM Dashboard with the Federal CDM Dashboard.

The Department established its Continuous Monitoring Plan, which outlined its continuous monitoring process at the information system level, as described in the ISCM Enterprise Roadmap. Based on our review of the plan, we determined that the Department defined ISCM metrics for Hardware Asset Management, Software Asset Management, Configuration Settings Management, and Vulnerability Management.

Both the Department and FSA established their own security assessment process for their respective systems. We obtained the system schedule for both processes and

determined that all nine judgmentally selected systems were included in both the Department's and FSA's processes and had current authorizations to operate.

Our review of various ISCM documents showed that roles and responsibilities were defined for key officials. ISCM stakeholders met to discuss ISCM matters, along with other Departmental programs, during quarterly Risk Management Framework Workshops, quarterly Cybersecurity Forums (which occur between quarterly Risk Management Framework Workshops), and monthly Cybersecurity Framework Risk Scorecard discussions.

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 and FSA 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 several areas needing improvement for this metric domain.

Finding 6. The Department and FSA's ISCM Program Needs Improvement

We found for the ISCM metric domain, the Department and FSA were at the Defined level for all five metric questions. We determined the Department and FSA's controls needed improvement for fully implementing ISCM strategy and policies, fully implementing its CDM program, and ensuring data accuracy in the Cybersecurity Framework Risk Scorecard.

ISCM Strategy and Policies Were Not Fully Implemented

Although the Department developed and communicated its ISCM Enterprise Roadmap inclusive of all required components and used a monthly Cybersecurity Framework Risk Scorecard to monitor and communicate high level risks, it did not consistently or effectively implement its strategy to collect and monitor of all defined metrics for its operational systems. For our nine judgmentally selected systems, we found that the Department did not (1) maintain monthly hardware and software inventory reports in the Cyber Security Assessment and Management tool for eight systems; (2) maintain monthly vulnerability scanning and monthly configuration setting results reports in the Cyber Security Asset and Management tool for all nine systems; and (3) develop system specific continuous monitoring plans for four systems. In addition, the Department did not fully provide oversight for all its external systems to ensure that external systems were also subjected to the Department's continuous monitoring processes. The

Department's efforts and resources were prioritized towards the PIVOT environment transition activities and the Cyber Security Asset and Management implementation. By implementing an automated security control process, the Department can help ensure that it maintains an effective ISCM program for its security controls. We reported a similar condition in our FY 2017 and FY 2018 FISMA audits.

DHS Continuous Diagnostics and Mitigation Program Not Fully Implemented

Although the Department made progress in implementing DHS CDM Phase components, such as the completing the CDM Federal Dashboard integration, it had not implemented of Phase 1 and Phase 2 of the program. Also, the Department completed the alignment of its information security continuous monitoring policies with the DHS CDM program; however, we found the Department had not consistently implemented the metrics for all nine of the judgmentally selected systems. In addition, the Department was not able to provide evidence of how it continuously monitors activities of external systems not included in the Department's CDM dashboard for four of the nine judgmentally systems. By not fully implementing a CDM program, the Department cannot ensure that security controls are adequately monitored to help protect its information technology assets and information. We reported a similar condition in our FY 2017 and FY 2018 FISMA audits.

Cybersecurity Framework Risk Scorecard Data Were Not Accurate

Data reported in the Cyber Security Assessment and Management tool were not always accurately reflected in the Cybersecurity Framework Risk Scorecard. The Department used Microsoft's Power BI tool[13] to extract data from the Cyber Security Assessment and Management tool that is used in populating its Cybersecurity Framework Risk Scorecard. We reviewed and compared data in the Cyber Security Assessment and Management tool to data reported in Power BI for July 1, 2019. Our comparison identified two systems reported in the Cyber Security Assessment and Management tool classified as FISMA reportable; however, in Power BI, these same systems were identified as non-FISMA reportable. The Department used a manual process to transfer data from the Cyber Security Assessment and Management tool to Power BI. Further, this process was not real-time and extracted data only at the first of the calendar month. Without an effective and timely process to transfer data from the Cyber Security Assessment and Management tool to Power BI, there is an increased risk the Department will rely on inaccurate data when reporting on its Cybersecurity Framework Risk Scorecard that is used to make informed risk decisions.

[13] Power BI is a business analytics service that provides interactive visualizations and business intelligence capabilities for end users to create their own reports and dashboards.

NIST SP 800-137, "Information Security Continuous Monitoring for Federal Information Systems and Organizations," requires that agencies define and implement an organization wide ISCM strategy that addresses risk at each organizational tier (organization, mission/business, and information system). It also states that part of the implementation stage of the continuous monitoring process is effectively organizing and delivering ISCM data to stakeholders in accordance with decision-making requirements. The Department's Continuous Monitoring Plan also states that each system information system security officer is required to report monthly on the Vulnerability Management and Configuration Settings Management metrics and report quarterly on Hardware Asset Management/Software Asset Management metrics. In addition, the Department's ISCM Roadmap states that information security officers are responsible for developing continuous monitoring plans for each information system.

Without a fully implemented ISCM strategy, the Department will not be able to ensure the timely collection of established metrics across operational systems, giving ISCM stakeholders and management an accurate representation of the status of its ISCM program to make informed risk-based decisions. Also, without complete implementation of the DHS CDM program, the Department will not be able to leverage the monitoring capabilities and tools to manage its systems and ultimately achieve a more effective ISCM program.

Recommendations

We recommend that the Deputy Secretary and the Chief Operating Officer require OCIO and FSA to—

6.1 Incorporate additional measures to, at a minimum; achieve Level 3 Consistently Implemented status of the ISCM program.

We recommend that the Deputy Secretary require OCIO to—

6.2 Automate its capabilities for monitoring the security controls effectiveness and overall implementation of the ISCM Roadmap. (Repeat Recommendation)

6.3 Ensure the completion of Phases 1 and 2 of the CDM program. (Repeat Recommendation)

6.4 Implement a process that ensures data reported on the Cybersecurity Framework Risk Scorecard is accurate.

Management Comments

The Department concurred with (1) Recommendation 6.1 and expects to close the FY 2018 corrective action associated with the recommendation by September 30, 2021; (2) Recommendation 6.2 and expects to close the FY 2018 corrective action associated

with the recommendation by October 30, 2020; (3) Recommendation 6.3 and expects to close the FY 2018 corrective action associated with the recommendation by January 29, 2021; and (4) Recommendation 6.4, and will develop a corrective action plan by December 31, 2019 to address the recommendation.

OIG Response

OIG will continue to monitor the Department's progress in closing out recommendations 6.1, 6.2, and 6.3. For 6.4, OIG 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 2020 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 Defined level of the maturity model, which is considered not effective. We found that the Department continued to develop and strengthen its incident response program. FSA established policies and procedures consistent with NIST guidelines and OMB policy; established an incident response process, participated in the DHS EINSTEIN program[14]; deployed numerous incident response tools; and established a process for enterprise level incident reporting requirements. However, we noted that improvements are needed in the Department's to help the agency reach a higher level of maturity. For instance, we found categorizing and reporting incidents to the United States Computer Emergency Readiness Team and OIG needed improvement and ensuring that data loss prevention tools are working as intended.

METRIC DOMAIN 7—INCIDENT RESPONSE

We determined that the Department's incident response program was consistent with the Defined 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 information technology 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

[14] The EINSTEIN program is an automated process for collecting, correlating, analyzing, and sharing computer security information across the Federal civilian government.

demonstrate the impact of the Department's cyber defense approach, its cyber state, and cyber security posture.

The Department established policies, procedures, and guidance to define its incident response process.[15] These include areas of personally identifiable information breach response, incident escalation, containment strategies, the U.S. Computer Emergency Readiness Team reporting, digital forensics, event analysis, and chain of custody. The Department also established an enterprise-level Cybersecurity Incident Response Plan. In addition, the Department's Security Operations Center's incident handling and notification procedures follow the U.S. Computer Emergency Readiness Team notification and the NIST guidelines.

The Department established roles and responsibilities for incident management, including the Chief Information Security Officer and the Department's security operation centers. The Department also conducted annual reviews to identify missing roles and responsibilities. Security awareness training, quarterly incident response testing, and high value asset briefings also helped identify roles and responsibilities. Incident response issues were communicated to the Chief Information Officer and Deputy Chief Information Officer through a weekly cyber report, as well as daily Department Security Operations Center meetings used to review all current and open incidents.

The Department implemented various incident response tools and technologies (intrusion detection, intrusion prevention, and data loss prevention) to assist in detecting and analyzing threats. For instance, it could identify whether internet protocol addresses or domains are identified as being malicious; which internet service provider, business, or country the internet protocol address was registered in; and whether an internet protocol address or domain was blacklisted. For denial of service attacks, the Department relied on Managed Trusted Internet Protocol Services. The Department also participated in the deployment of DHS' EINSTEIN Intrusion Prevention Security Services on its network to identify traffic indicating known or suspected malicious cyber activity.

The Department's incident response training was provided through its Cybersecurity and Privacy Awareness training, as well as role-based training. Through its training program, the Department improved its phishing detection. Specifically, in its most recent phishing exercise, 6,589 of 6,593 (99.93%) of network users successfully passed

[15] Previous Departmental guidance addressing incident response, HB OCIO-14, Handbook for Cybersecurity Incident Response and Reporting, was superseded by HB OCIO 3-112, Cybersecurity Policy.

the exercise, and 1,834 users reported the phishing email to the Department's Security Operations Center—the highest reporting rate to date.

However, its practices in all 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 had the ability to manage and measure the impact of successful incidents, 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 several areas needing improvement for this metric domain.

Finding 7. The Department's Incident Response Program Needs Improvement

We found that for the Incident Response metric domain, the Department was at the Consistently Implemented level for two metric questions, and the Defined level for five metric questions. We determined that the Department needed to improve controls for reporting incidents consistently to the OIG and ensuring data loss prevention tools worked as intended.

Incidents Were Not Consistently Reported to the OIG

According to the U.S. Computer Emergency Readiness Team Federal Incident Notification Guidelines, the Department's Security Operations Center must report information security incidents, where the confidentiality, integrity, or availability of a Federal information system is potentially compromised, within 1 hour of being identified by the agency's top-level Computer Security Incident Response Team, Security Operations Center, or information technology department. These requirements were incorporated into the Department's incident response policies and procedures.[16] The Department used a prioritization scale that identified different types of security incidents. The categories range from 1 to 6, with category 1 having the highest criticality. The same guidance further clarifies that the Department's Security Operations Center Coordinator ensures that the OIG Duty Agent is immediately notified for all the U.S. Computer Emergency Readiness Team Category 1 through 3 incidents, as well as other high visibility or on-going incidents.

[16] Standard RS.CO 1-Computer Crime Incident Reporting; and the U.S. Computer Emergency Readiness Team and OIG Reporting Procedures IAS-SOP-CO-200.

Between the October 1, 2018, and March 12, 2019, the Department incurred 1,324 security incidents ranging from Category 0 to 6. For 335 incidents categorized as Category 1 through 3, only 30 security incidents (or 9 percent) were reported to the OIG. We found instances where reporting to the OIG took more than 6 hours for Category 1 incidents—with one incident taking more than 32 days. We also found instances where reporting took more than 8 days for Category 3 incidents. We reviewed security incidents between March 13, 2019, and June 17, 2019, and found that the Department incurred 717 incidents ranging from Category 0 to 6. For the 155 incidents categorized as Category 1 through 3, only 4 security incidents (or 3 percent) were reported to the OIG. We also found one instance in Category 3 where reporting to OIG took more than 2 hours. In addition, we identified that for 3 Category 4 incidents—that the Department deemed reportable—took more than 4 hours. Failure to report these incidents impedes the OIG's ability to secure vital evidence, make important connections to ongoing cases, or make decisions about initiating new cases. We reported a similar condition in our FY 2017 and 2018 FISMA audits.

Data Loss Prevention Tool Did Not Consistently Function as Intended

The Department established a data loss prevention process designed to help prevent the disclosure of personally identifiable information or other sensitive data and relied on a variety of tools to detect and analyze these events. These tools included McAfee Data Loss Prevention and Online Protection Data Loss Prevention.[17] The Department's data loss prevention solution was host based and was located on all devices.

Although our testing found that the Department's data loss prevention solution was able to detect emails containing specific identifiers such as "SSN" and "Social Security Number," detecting unencrypted Social Security numbers or numeric strings remains a challenge for the Department. Specifically, we found that the Department's data loss prevention solution neither detected, nor stopped, multiple transmissions of unencrypted social security numbers along with personally identifiable information. We were able to transmit unencrypted information such as Social Security numbers, dates of birth, credit card information, names, personal addresses, and email addresses of test individuals across the Department's network to both inside and outside the organization. Although the Department's enterprise-wide data loss prevention solution policy is designed to identify and block the transmission of unencrypted social security numbers based on certain identifiers, it does not detect other identifiers that can circumvent the detection triggers and possibly allow the unauthorized disclosure of large volumes of personally identifiable information. Additionally, a recent examination by the OIG's Technology Crimes Division of an incident identified by the Department's

[17] McAfee will be replaced with Dell Endpoint protection in the new PIVOT environment.

data loss prevention tool. That incident initially appeared to involve unencrypted personally identifiable information being sent to an external recipient. However, further OIG assessment of the incident confirmed that the information identified did not contain Social Security numbers, names, addresses, or dates of birth, and it was determined to be a false positive. As a result, the OIG's Technology Crimes Division suggested that the Department's Security Operations Center needed to take appropriate steps to fine tune its data loss prevention detection algorithms and implement a data loss prevention alert corroboration process improvement. We identified this issue in our FY 2016 and FY 2017 FISMA audits.

OMB and NIST guidelines identify several requirements for implementing an effective incident response program.[18] Adhering to the guidelines allows for establishing policies and procedures, implementing technical controls, and implementing and enforcing coordinated security incident activities. 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 information technology systems or disclosure of sensitive data.

Recommendations

We recommend that the Deputy Secretary require OCIO to—

7.1 Incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Incident Response program.

7.2 Ensure that incidents are consistently submitted to the OIG within the required timeframe.

7.3 Ensure that data loss prevention technologies work as intended for the blocking of sensitive information transmission.

Management Comments

The Department concurred with Recommendation 7.1 and expects to close the FY 2018 corrective action associated with the recommendation by September 30, 2021. It also

[18] 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.

partially concurred with Recommendation 7.2 citing that OIG's Technology Crimes Division was provided with accounts allowing access to the Department's security operations incident management system and providing the ability to review all Department incidents. The Department also stated that if an incident is potentially criminal in nature, the Department's Security Operation Center will follow its Computer Crime Incident Reporting standard. It also stated that it will develop a corrective action plan by December 31, 2019 to address the recommendation. The Department also concurred with Recommendation 7.3 and stated that it will develop a corrective action plan by February 28, 2020.

OIG Response

OIG will continue to monitor the Department's progress in closing out Recommendation 8.1. For Recommendation 8.2, OIG agrees that providing the Technology Crimes Division access to the Department's security operations incident management system has provided the ability to review all Department's incidents. However, the Department's Security Operations Center may not have the ability to determine whether an incident occurred because of criminal intent. This determinization should be the responsibility of the Technology Crimes Division. Therefore, the Department needs to ensure that all artifacts are collected and obtained in a timely manner for the Technology Crimes Division to examine and make that determination. We request that this is included in your proposed corrective action plan. For Recommendation 8.3, we will review the corrective action plan to determine if the actions will address the finding and recommendation and if so, will validate corrective actions taken during our FY 2020 FISMA audit fieldwork.

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 completeness of the contingency plan documentation. See below for the details.

METRIC DOMAIN 8—CONTINGENCY PLANNING

We determined that the Department's and FSA's Contingency Planning programs were consistent with the Consistently Implemented level of the maturity model, which is considered not effective. We identified areas where the Department made improvements to its contingency planning program.

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.

The Department defined its policies, procedures, and strategies for its information system contingency planning and disaster recovery function. Roles and responsibilities for contingency planning were defined and communicated across the organization. Enterprise-wide and system specific plans, such as the Continuity of Operations Plan and Disaster Recovery Plan, identified roles and responsibilities for contingency planning. To ensure that these roles and responsibilities were performed, they were included as part of contingency plan testing. Since contingency plan testing impacts recovery scores on the Department's Cybersecurity Framework Risk Scorecard, it allowed principal offices, the Deputy Secretary, and the Secretary to identify systems with stakeholders that were not effectively carrying out their roles and responsibilities.

The Department established an enterprise-wide continuity plan that identified mission essential functions. It also established enterprise-wide templates for contingency plans, contingency plan testing, and disaster recovery plans. The Department maintained evidence of its contingency planning using the Cyber Security Assessment and Management tool. Our review of contingency plans showed that they included all stages of the contingency planning process—activation and notification, recovery, and reconstitution. Contingency plans include processes for system backup and storage, as well as the use of alternate storage and processing sites. Further, contingency plans integrated supply chain concerns. The Department also established a Business Impact Analysis Management Plan. A Business Impact Analysis was required as part of the contingency plan template, and we verified that analyses were being included through our review of active contingency plans.

The Department used POA&Ms to identify and track contingency planning deficiencies. The Capital Planning and Investment Control and Information Technology Review Committee reviewed the deficiencies during the Department's investment review process. Our review of POA&Ms confirmed that contingency planning deficiencies were being identified and tracked for Departmental systems.

We also reviewed system security plans maintained in the Cyber Security Assessment and Management tool and verified that contingency planning elements were included in the plans. These elements included establishing an alternate storage site; maintaining alternate storage agreements; maintaining information security safeguards equivalent to the primary site; system backup frequency; backup of information system documentation; and protecting the confidentiality, integrity, and availability of backup information at storage locations.

The Department maintained system contingency planning test plans that included testing elements such as notification procedures, system recovery on an alternate platform from backup media, internal and external connectivity, and coordination with other business areas. It also coordinated annual contingency plan testing with external service providers and supply chain partners. Our review of contingency planning test plans found no deficiencies relating to missing elements.

The Department monitored contingency plan testing dates using the Cyber Security Assessment and Management tool. Contingency planning test dates were reportable items on the Cybersecurity Risk Scorecard. These scorecards were reviewed monthly to monitor whether plans were being tested and whether stakeholders' roles and responsibilities were incorporated as part of testing.

Quarterly Cyber Operations Tabletop exercises were conducted to provide system owners the ability to test their contingency plans, determine the effectiveness of the plans and identify potential weaknesses. Activity was tracked and measured against standard operating procedures. Further, training analysts and recorders provided their results as input to the after-action report. These reports enabled Information System Security Officers and system owners to make changes and updates based on the results.

Despite these actions, 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 and FSA 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 documented and updated. Finding 8 identifies several areas needing improvement for this metric domain.

Finding 8. The Department and FSA's Contingency Program Needs Improvement

We found that for the Contingency Planning metric domain, the Department and FSA were at the Defined level for three metric questions, and at the Consistently Implemented level for four metric questions. We determined the Department and FSA's controls for documenting and updating their contingency plans needed improvement.

Contingency Plans Were Not Consistently Documented and Updated

Although the Department established and maintained an enterprise-wide business continuity and disaster recovery program, we found the Department did not consistently and timely document its contingency planning information. Overall, we found that of 120 Departmental and FSA systems, 34 did not have current system contingency plans. Further, for the 120 systems, 21 system contingency plans were not

located in Cyber Security Assessment and Management tool. We judgmentally selected nine systems for review and could not locate contingency plans for three of them.

To ensure that contingency plans reflect the most current requirements, the Department relied on other system artifacts such as risk assessments, system security plans, privacy impact assessments, privacy threshold analyses, business impact analyses, disaster recovery plans, and incident response plans. For nine judgmentally selected systems, we found that (1) eight risk assessments were not documented; (2) seven system security plans were not current; (3) nine did not have documented Privacy Impact Assessments or documented Privacy Threshold Analyses; (4) eight had significantly outdated Business Impact Assessments—dating back to 2013; (5) six did not have a current disaster recovery plan; and (6) two did not have a current incident response plan. Although the Department uses the Cyber Security Assessment and Management tool to maintain a central repository for all its information system documentation, the tool did not have automated capabilities for the Department's contingency planning documentation.

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 establishing contingency plans and contingency plan testing. 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 its information technology resources in the event of a disaster. We reported similar conditions in our FY 2012, 2014, 2015, and 2018 FISMA audits.

Recommendations

We recommend that the Chief Operating Officer require FSA to—

8.1 Incorporate additional measures to, at a minimum; achieve Level 4 Managed and Measurable status of the Contingency Planning program.

8.2 Ensure that contingency plans, and other artifacts impacting contingency plans, are documented and updated in a consistent and timely manner.

Management Comments

The Department concurred with Recommendation 8.1 and expects to close the FY 2018 corrective action associated with the recommendation by September 30, 2021. For Recommendation 8.2, the Department concurred and will develop a corrective action plan by December 31, 2019, to address the recommendation.

OIG Comments

OIG will continue to monitor the Department's progress in closing out Recommendation 8.1. Further, it will review the corrective action plan for Recommendation 8.2 to determine if the actions will address the finding and recommendation and if so, will validate during our FY 2020 FISMA audit fieldwork.

Appendix A. Scope and Methodology

For FY 2019, the Inspector General 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 information technology security controls by reviewing policies, procedures, and practices that the Department implemented at the enterprise and levels
- assessed the Department's enterprise and system-level security controls;
- interviewed Department officials and contractor personnel, specifically staff with information technology 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 DHS' FY 2019 IG FISMA Metrics; 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 Configuration Management and Contingency Planning metric domains;
- reviewed corrective action plans identified starting from January 2019 through July 2019;
- identified and verified systems required to use a trusted internet connection;
- tested websites for encryption protocol, masking of personally identifiable information, use of Social Security numbers, and use of website banners;

- tested and reviewed authorized active connections for security connection protocols;
- identified users who did not take required security training from October 2018 through February 2019;
- reviewed computer security incidents that were reported from October 1, 2018 through June 17, 2019;
- performed vulnerability assessments of applications for Enterprise Data Warehouse Analytics; myStudentAid[19]; National Student Loan Database System; Central Processing System; Debt Management Collection System 2; Department of ED/Perkins; Great Lakes Commercial System; and Nelnet Servicing;
- verified training evidence and completion; and
- verified security settings for Department data protection.

Sampling Methodology

As of February 2019, the Department identified an inventory of 142 systems that were FISMA reportable and classified as operational. Of the 142 FISMA reportable systems 3 were classified as high, 98 as moderate, and 41 as low-impact systems.

During the PIVOT transition, Department systems did not reside in a static environment where the testing of technical controls may produce consistent or accurate results. Because of the delayed transition of Department systems to the PIVOT hosting environment, we focused our system testing on FSA systems. We judgmentally selected 9 of 59 FSA systems that were externally hosted or resided within the Next Generation Data Center hosting environment.

In making our selection, we considered risk-based characteristics such as system classifications (high, moderate, and low), those systems externally hosted, systems made fully operational within the prior 3 years, and systems classified as high-value assets.

[19] A student aid phone application used on both iPhone and Android devices. This was the first time the OIG has performed testing on this type of device.

The table below lists the judgmentally selected systems, the system's principal office, and the Federal Information Processing Standards Publication 199 potential impact level.[20]

Table 4. Listing of Systems Reviewed

Number	System Name	Impact Level
1	Education Data Warehouse Analytics	Moderate
2	myStudentAid	Moderate
3	National Student Loan Database System	Moderate
4	Central Processing System	Moderate
5	Debt Management Collection System 2	Moderate
6	Department of ED/Perkins	Moderate
7	Great Lakes Commercial System	Moderate
8	Pennsylvania Higher Education Assistance Authority	Moderate

[20] 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.

9	Nelnet Servicing	Moderate

Testing of these systems helped us ascertain the security control aspects relating to Configuration Management and Contingency Planning.[21] In addition, these systems were the focus of our system vulnerability assessment and testing.

For reviewing access agreements, we judgmentally selected 15 new users (10 from Departmental offices and 5 from FSA systems tested during the audit). For role-based training, we judgmentally selected 28 FSA contractors with privileged access.

For new user access, we received a list of 590 new users that started employment with the Department from October 2018 through February 2019, we judgmentally selected 10 new users (4 Department employees and 6 contractors).

Use of Computer-Processed Data

For this audit, we reviewed the security controls and configuration settings for vendor systems and applications externally hosted and systems residing at the Next Generation Data Center hosting environment. We used computer-processed data for the 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 or generated through a system where auditors did not have rights to access the system. 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. The computer-processed data were verified to source data and tested for accuracy according to relevant system controls until enough information was available to make a reliability determination. For instance, we performed (1) logical tests; (2) comparisons of values to validate a logical or defined correlation; (3) tests for duplicate entries, missing data, and values outside of designated ranges or timeframes; (4) tests using analyzation tools; and (5) comparison of the data with Department scorecards.

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

We conducted our fieldwork from February 2019 through August 2019, primarily at Department offices in Washington, D.C. We conducted an exit conference with Department and FSA officials on October 28, 2019.

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. The evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix B. System Reassessment, Program Realignment, and Policy Implementation

System Reassessment

The Common Origination and Disbursement system processes federal financial aid programs for the Department by integrating eligible school and borrower participation across the financial aid programs by providing a consolidated, comprehensive set of tools for each set of users. This toolset also provides data to financial aid partners, services, and FSA. The Common Origination and Disbursement communicates with multiple systems to send and receive data from major internal systems within its boundary including the Enterprise Data Warehouse and Analytics system. This system is a data warehouse for FSA users and is used for data requests, reporting, and analytics initiatives. The Enterprise Data Warehouse and Analytics system receives data from various systems regarding sensitive financial and student information such as (1) the Central Processing System—that processes data submitted on Free Application for Federal Student Aid; (2) the Financial Management System—a financial accounting system that stores all financial information for FSA processing, including financial transaction information processed by the Common Origination and Disbursement system; (3) the Enterprise Complaints System—used for providing analytics insights and dashboards for cases and contracts; and (4) commercial loan servicers. In addition, the Department lists the Enterprise Data Warehouse and Analytics system as a major information technology investment.

Although the Enterprise Data Warehouse and Analytics system is located within the Common Origination and Disbursement system boundary, because it stores data from various systems processing financial and personally identifiable information in a centralized location, there is a high risk associated with the system in the event it becomes compromised allowing the exfiltration of data. Because of the risk associated with centralizing sensitive data from different systems into a single system, separate controls commensurate with this risk needs to be established for the Enterprise Data Warehouse and Analytics system. This concern is further recognized by our vulnerability assessment and penetration testing results identifying a high priority vulnerability.

Data Privacy and Protection Realignment

As a result of a reorganization effort, the responsibility of the Department's Data Protection and Privacy Program was assigned to the Cyber Operations Branch of the

Information Assurances Services[22] component of the OCIO. This alignment allowed for better integration with the Department's cybersecurity effort to assist in better oversight of the program and the ability to identify opportunities for improvement. The Cyber Operations Branch establishes and implements the operational processes for detecting, protecting and responding to cybersecurity threats and vulnerabilities and provides leadership, oversight, and coordination for the Department's privacy program. Specifically, this branch is responsible for (1) establishing and maintaining a comprehensive privacy program that ensures compliance with applicable privacy and breach notification requirements; (2) developing and evaluating Department-wide privacy policies; (3) promoting privacy awareness and education across the Department; (4) providing guidance and instruction to Departmental staff regarding processes and procedures involving the protection of personally identifiable information; and (5) overseeing the implementation and management of Department-wide systems and databases supporting the successful handling of privacy safeguards administration.

In 2018, FSA completed an initiative to determine the extent of sensitive data that included personally identifiable information. The results were intended to assist in establishing the framework to develop a formal Department-wide assessment process. The effort will assist in establishing a baseline, improve decision-making and overall privacy response, and strengthening the data loss prevention process.

Cybersecurity Policy Framework Implementation

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 Information Assurance Services Division replaced existing Departmental cybersecurity guidance with policies, instructions and standards that align to the National Institute of Standards and Technology 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. Also, beginning in January 2019, existing Departmental cybersecurity guidance documents were being replaced through formal Instructions, standards, procedures, and guidance that align with the Cybersecurity Framework.

[22] The mission of the Information Assurances Services component is to oversee the Department's security program and ensure the confidentiality/privacy, integrity and availability of the Department's information and information resources.

Appendix C. CyberScope FY 2019 IG FISMA Metrics

For Official Use Only

Inspector General
Section Report

2019
Annual FISMA
Report

Department of Education

For Official Use Only

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 CM8; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2019 CIO FISMA Metrics: 1.1 and 1.4, OMB A-130).

Defined (Level 2)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 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 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 2019 CIO FISMA Metrics: 1.2 and 3.9.2; CSF: ID.AM-1).

Defined (Level 2)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 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: CA7, CM-8, and CM-10; NIST SP 800-137; NISTIR 8011; FEA Framework, v2; FY 2019 CIO FISMA Metrics: 3.10.1; CSF: ID.AM-2)?

Defined (Level 2)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 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 PM11; NIST SP 800-60; NIST SP 800-37 (Rev. 2); CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2019 CIO FISMA Metrics: 1.1; OMB M-19-03)?

Consistently Implemented (Level 3)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 1:The Department's Risk Management Program Needs Improvement

For Official Use Only

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)?

Defined (Level 2)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 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 (NIST SP 800-39; NIST SP 800-160; NIST SP 800-37 (Rev. 2); OMB M-19-03; FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA9, SA-12, and PM-9; NIST SP 800-161; CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?

Defined (Level 2)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 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 M19-03)?

Defined (Level 2)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 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)?

Defined (Level 2)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 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))?

Defined (Level 2)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 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: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 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: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 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: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 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?

U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019
ED-OIG/A11T0002 (FISMA Report) Issue 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)?

Consistently Implemented (Level 3)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 2:The Department and FSA's Configuration Management Program Needs Improvement

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)?

Defined (Level 2)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 2:The Department and FSA's Configuration Management Program Needs Improvement

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: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 2:The Department and FSA's Configuration Management Program Needs Improvement

Function 2A: Protect - Configuration Management

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 2019CIO FISMA Metrics: 1.1,2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7and PR.IP-1)?

Defined (Level 2)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 2:The Department and FSA's Configuration Management Program Needs 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, and SI-2; FY 2019CIO FISMA Metrics: 1.1 and 2.2; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1and DE.CM-8)?

Defined (Level 2)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 2:The Department and FSA's Configuration Management Program Needs Improvement

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 and SI-2; NIST SP 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20,Control 4.5; FY 2019CIO FISMA Metrics: 2.13; CSF: ID.RA-1; DHS Binding Operational Directive(BOD)15-01; DHS BOD 18-02)?

Defined (Level 2)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 2:The Department and FSA's Configuration Management Program Needs Improvement

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-08-05)?

Defined (Level 2)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 2:The Department and FSA's Configuration Management Program Needs Improvement

Function 2A: Protect - Configuration Management

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 and CM-3; CSF: PR.IP-3).?

Consistently Implemented (Level 3)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 2:The Department and FSA's Configuration Management Program Needs 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?

U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 2:The Department and FSA's Configuration Management Program Needs Improvement

Calculated Maturity Level - Defined (Level 2)

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/A11T0002 (FISMA Report) Issue 3: The Department and FSA'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/A11T0002 (FISMA Report) Issue 3: The Department and FSA's Identity and Access Management Program Needs Improvement

Function 2B: Protect - Identity and Access Management

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/A11T0002 (FISMA Report) Issue 3: The Department and FSA'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/A11T0002 (FISMA Report) Issue 3: The Department and FSA'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/A11T0002 (FISMA Report) Issue 3: The Department and FSA's Identity and Access Management Program Needs Improvement

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/A11T0002 (FISMA Report) Issue 3: The Department and FSA's Identity and Access Management Program Needs Improvement

Function 2B: Protect - Identity and Access Management

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)?

Ad Hoc (Level 1)

Comments: ED-OIG/A11T0002 (FISMA Report) Issue 3: The Department and FSA'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/A11T0002 (FISMA Report) Issue 3: The Department and FSA'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)?.

Defined (Level 2)

Comments: ED-OIG/A11T0002 (FISMA Report) Issue 3: The Department and FSA's Identity and Access Management Program Needs Improvement

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/A11T0002 (FISMA Report) Issue 3: The Department and FSA's Identity and Access Management Program Needs Improvement

Calculated Maturity Level - Defined (Level 2)

Function 2C: Protect - Data Protection and Privacy

For Official Use Only

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/A11T0002 (FISMA Report) Issue 4: The Department and FSA'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/A11T0002 (FISMA Report) Issue 4: The Department and FSA'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/A11T0002 (FISMA Report) Issue 4: The Department and FSA'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)?

Defined (Level 2)

Comments: ED-OIG/A11T0002 (FISMA Report) Issue 4: The Department and FSA's Data Protection and Privacy Program Needs Improvement

Function 2C: Protect - Data Protection and Privacy

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/A11T0002 (FISMA Report) Issue 4: The Department and FSA's Data Protection and Privacy Program Needs Improvement

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/A11T0002 (FISMA Report) Issue 4: The Department and FSA'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/A11T0002 (FISMA Report) Issue 5: The Department and FSA'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/A11T0002 (FISMA Report) Issue 5: The Department and FSA's Security Training Program Needs Improvement

Function 2D: Protect - Security Training

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/A11T0002 (FISMA Report) Issue 5: The Department and FSA's Security Training Program Needs Improvement

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/A11T0002 (FISMA Report) Issue 5: The Department and FSA'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).

Defined (Level 2)

Comments: ED-OIG/A11T0002 (FISMA Report) Issue 5: The Department and FSA'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/A11T0002 (FISMA Report) Issue 5: The Department and FSA'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/A11T0002 (FISMA Report) Issue 5: The Department and FSA's Security Training Program Needs Improvement

Function 2D: Protect - Security Training

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?

ED-OIG/A11T0002 (FISMA Report) Issue 5: The Department and FSA's Security Training Program Needs Improvement

Calculated Maturity Level - Defined (Level 2)

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/A11T0002 (FISMA Report) Issue 6: The Department and FSA's Information Security Continuous Monitoring 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/A11T0002 (FISMA Report) Issue 6: The Department and FSA's Information Security Continuous Monitoring Program Needs Improvement

48 To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined 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)?.

Defined (Level 2)

Comments: ED-OIG/A11T0002 (FISMA Report) Issue 6: The Department and FSA's Information Security Continuous Monitoring Program Needs Improvement

Function 3: Detect - ISCM

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)

Defined (Level 2)

Comments: ED-OIG/A11T0002 (FISMA Report) Issue 6: The Department and FSA's Information Security Continuous Monitoring Program Needs Improvement

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

Defined (Level 2)

Comments: ED-OIG/A11T0002 (FISMA Report) Issue 6: The Department and FSA's Information Security Continuous Monitoring Program Needs Improvement

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

Defined (Level 2)

Comments: ED-OIG/A11T0002 (FISMA Report) Issue 6: The Department and FSA's Information Security Continuous Monitoring Program Needs Improvement

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/A11T0002 (FISMA Report) Issue 6: The Department and FSA's Information Security Continuous Monitoring 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).

Defined (Level 2)

Comments: ED-OIG/A11T0002 (FISMA Report) Issue 7: The Department and FSA's Incident Response Program Needs Improvement

Function 4: Respond - Incident Response

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)?

Defined (Level 2)

Comments: ED-OIG/A11T0002 (FISMA Report) Issue 7: The Department and FSA'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/A11T0002 (FISMA Report) Issue 7: The Department and FSA'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/A11T0002 (FISMA Report) Issue 7: The Department and FSA's Incident Response Program Needs Improvement

56 To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-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/A11T0002 (FISMA Report) Issue 7: The Department and FSA'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).

Consistently Implemented (Level 3)

Comments: ED-OIG/A11T0002 (FISMA Report) Issue 7: The Department and FSA's Incident Response Program Needs Improvement

For Official Use Only

Function 4: Respond - Incident Response

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)

Defined (Level 2)

Comments: ED-OIG/A11T0002 (FISMA Report) Issue 7: The Department and FSA's Incident Response Program Needs Improvement

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

Defined (Level 2)

Comments: ED-OIG/A11T0002 (FISMA Report) Issue 7: The Department and FSA'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/A11T0002 (FISMA Report) Issue 7: The Department and FSA's Incident Response Program Needs Improvement

Calculated Maturity Level - Defined (Level 2)

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/A11T0002 (FISMA Report) Issue 8: The Department and FSA'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/A11T0002 (FISMA Report) Issue 8: The Department and FSA's Contingency Planning Program Needs Improvement

Function 5: Recover - Contingency Planning

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)?

Defined (Level 2)

Comments: ED-OIG/A11T0002 (FISMA Report) Issue 8: The Department and FSA'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/A11T0002 (FISMA Report) Issue 8: The Department and FSA'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/A11T0002 (FISMA Report) Issue 8: The Department and FSA'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/A11T0002 (FISMA Report) Issue 8: The Department and FSA's Contingency Planning Program Needs Improvement

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)?

Defined (Level 2)

Comments: ED-OIG/A11T0002 (FISMA Report) Issue 8: The Department and FSA'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/A11T0002 (FISMA Report) Issue 8: The Department and FSA's Contingency Planning Program Needs Improvement

Function 5: Recover - Contingency Planning

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/A11T0002 (FISMA Report) Issue 8: The Department and FSA'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

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 Department of Education's (Department) and Federal Student Aid's (FSA) overall information technology security programs and practices were effective as they relate to Federal information security requirements. We assessed the effectiveness of security controls based on the extent to which the controls were implemented correctly, operated as intended, and producing the desired outcome with respect to meeting the security requirements for the information systems we review in their operational environment. We found that the Department and FSA were not effective in any of the five security functions—Identify, Protect, Detect, Respond, and Recover. We also identified findings in all eight metric domains. The Department has made improvements on individual metric scoring (questions). The Department demonstrated improvement from FY 2018 within the metric areas 1.) Security Training 2.) Identity and Access Management 3.) Configuration Management 4.) Data Privacy and Protect 5.) Contingency Planning and 6) Incident Response. The most significant change was in Risk Management. The overall maturity rating for the security function went from Consistently Implemented to Defined. This was due to the new requirements in this year's FY 2019 FISMA IG Metrics addressing the SECURE Technology Act provisions for supply chain management, as well as related policy and procedural requirements. Except for Risk Management, the overall FY 2019 maturity level rating was not impacted.

APPENDIX A: Maturity Model Scoring

Function 1: Identify - Risk Management

Function	Count
Ad-Hoc	0
Defined	10
Consistently Implemented	1
Managed and Measurable	0
Optimized	1
Function Rating: Defined (Level 2)Not Effective	

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	0
Defined	6
Consistently Implemented	2
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)Not Effective	

Function 2B: Protect - Identity and Access Management

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

Function 2C: Protect - Data Protection and Privacy

Function	Count
Ad-Hoc	0
Defined	5
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)Not Effective	

Function 2D: Protect - Security Training

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

Function 3: Detect - ISCM

Function	Count
Ad-Hoc	0
Defined	5
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)Not Effective	

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	5
Consistently Implemented	2
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)Not Effective	

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	0
Defined	3
Consistently Implemented	4
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)	U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2019 ED-OIG/A11T0002 (FISMA Report) Issue 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/A11T0002 (FISMA Report) Issue 5: The Department and FSA's Security Training Program Needs Improvement
Function 3: Detect - ISCM	Defined (Level 2)	Defined (Level 2)	ED-OIG/A11T0002 (FISMA Report) Issue 6: The Department and FSA's Information Security Continuous Monitoring Program Needs Improvement
Function 4: Respond - Incident Response	Defined (Level 2)	Defined (Level 2)	ED-OIG/A11T0002 (FISMA Report) Issue 7: The Department and FSA's Incident Response Program Needs Improvement
Function 5: Recover - Contingency Planning	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	ED-OIG/A11T0002 (FISMA Report) Issue 8: The Department and FSA's Contingency Planning Program Needs Improvement
Overall	Not Effective	Not Effective	

Appendix D. Acronyms and Abbreviations

CDM	Continuous Diagnostics and Mitigation
Department	U.S. Department of Education
DHS	Department of Homeland Security
EDUCATE	Education Department Utility for Communications, Applications, and Technology Environment
FISMA	Federal Information Security Modernization Act of 2014
FSA	Federal Student Aid
FY	fiscal year
ICAM	Identity, Credential, and Access Management
ISCM	Information Security Continuous Monitoring
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
PIVOT	Portfolio of Integrated Value-Oriented Technologies
POA&M	Plan of Action and Milestones
SP	Special Publication

Department and FSA Comments

UNITED STATES DEPARTMENT OF EDUCATION

DATE: October 30, 2019

TO: Robert D. Mancuso
Assistant Inspector General
Information Technology Audits and Computer Crime Investigations
Office of Inspector General

FROM: Mick Zais
Deputy Secretary
Department of Education

Mark A. Brown
Chief Operating Officer
Federal Student Aid

SUBJECT: Response to Discussion Draft Audit Report
The U.S. Department of Education's Federal Information Security Modernization Act of 2014 for Fiscal Year 2019
Control Number ED-OIG/A11T0001

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) Report, Audit of the U.S. Department of Education's (the Department's) Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year (FY) 2019 Draft Report, Control Number ED-OIG/A11T0001. 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.

While the Department appreciates the work of the OIG on this audit, we wish to note at the outset that some of the work is long-term in nature, and the frequency of this annual audit often does not fully recognize the time needed to implement fully multi-year strategic planned improvements, programs, and capabilities. As demonstrated in the responses below, the Department has already been working toward completing 18 of the 37 total OIG recommendations through documented corrective actions in response to the OIG's FY 2018 audit, A11-S0001. The Department has also submitted to the OIG evidence of completion for five of the 35 recommendations. The Department does not concur with two of the 37 recommendations (*i.e.*, Recommendations 2.7, and 2.8). The remaining recommendations will be addressed through corrective action plans developed by the Office of the Chief Information Officer (OCIO).

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

REPORTING METRIC DOMAIN No. 1: RISK MANAGEMENT

The OIG recommends that the Deputy Secretary and Chief Operating Officer require that OCIO and FSA:

OIG Recommendation 1.1: Incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Risk Management program.

Management Response: The Department partially concurs with this recommendation. The Department believes there is simply a fundamental difference of opinion on the scoring methodology of this metric domain. As the table below demonstrates, Plan of Action and Milestones (POA&Ms) management at the Department has been a key focus area in FY 2019 and continues to be a critical component of our Risk Management Program. The Department has reduced the total POA&Ms by more than 83 percent and delayed POA&Ms by 95 percent.

Category	10/1/2018	10/1/2019	Delta	% Delta
Total POA&Ms	2,998	498	-2,500	-83.39%
Delayed POA&Ms	856	38	-818	-95.56%
Very High POA&Ms	723	123	-600	-82.99%
High POA&Ms	1,071	129	-942	-87.96%
Medium POA&Ms	872	202	-670	-76.83%
Low POA&Ms	247	42	-205	-83.00%
Total HVA POA&Ms	544	127	-417	-76.65%
CSAM Discrepancies	558	76	-482	-86.38%

The Department expects to take all necessary steps to fully respond to this finding and to be able to close the FY 2018 corrective action associated with this recommendation by September 30, 2021.

OIG Recommendation 1.2: Ensure that POA&M remediation is performed with in the required timeframe.

Management Response: The Department partially concurs with this recommendation. As noted in the response to Recommendation 1.1, the Department has made significant progress in resolving outdated POA&Ms. The Department will continue this effort in FY 2020 and will develop a corrective action plan by December 31, 2019, to address the recommendation.

OIG Recommendation 1.3: Ensure that all POA&Ms are assigned with the required appropriate remediation official.

Management Response: The Department partially concurs with this recommendation. Of the 830 POA&Ms identified by the IG, 815 were created and closed in FSA's previous POA&M system of record. In FY 2016, the Department completed the data migration to Cyber Security Assessment and Management (CSAM), the Department's and FSA's POA&M system of record. During this data migration the 'Assigned To' field did not populate for a number of POA&Ms for various reasons beyond OCIO's control. Of the remaining 15 POA&Ms, eight POA&Ms were created in error and procedurally closed prior to all fields being completed. To resolve this issue, FSA has added the remediation official for the remaining seven POAMs and conducted internal training to ensure this information is added to all future POA&Ms. Evidence of this remediation was provided to the IG of this action for their review.

REPORTING METRIC DOMAIN No. 2: CONFIGURATION MANAGEMENT

The OIG recommends that the Deputy Secretary and Chief Operating Officer require that OCIO and FSA:

OIG Recommendation 2.1: Incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Configuration Management program.

Management Response: The Department concurs with this recommendation. The Department expects to take all necessary steps to fully respond to this finding and to be able to close the FY 2018 corrective action associated with this recommendation by September 30, 2021.

OIG Recommendation 2.2: Migrate to Transport Layer Security 1.2 or higher as the only connection for all Department connections.

Management Response: The Department concurs with this recommendation. The Department has made significant progress in this area and expects to be able to close the FY 2018 corrective action associated with this recommendation by February 28, 2020.

OIG Recommendation 2.3: Review new solutions to assure that the default username and password has been changed.

Management Response: The Department concurs with this recommendation. Once notified of the vulnerability by the OIG, the Department immediately requested remediation by the service provider and issued a contractual letter of concern. Evidence of this remediation was provided to the IG of this action for their review.

The OIG recommends that the Deputy Secretary require OCIO to:

OIG Recommendation 2.4: Ensure that 51 websites are routed through a trusted internet connection or managed trusted internet protocol service.

Management Response: The Department concurs with this recommendation. The Department expects to complete the necessary corrective actions and to be able to close the FY 2018 corrective action associated with this recommendation by October 30, 2020.

OIG Recommendation 2.5: Ensure that all existing websites and services are accessible through a secure connection as required by OMB M-15-13.

Management Response: The Department concurs with this recommendation. The Department has continued to work with both the Department of Homeland Security (DHS) and vendors to resolve outstanding issues. As noted in the report, the Department has made progress on this item and expects to be able to close the associated FY 2018 corrective action by February 28, 2020.

The OIG recommends that the Chief Operating Officer require FSA to:

OIG Recommendation 2.6: Discontinue the use of unsupported operating systems, databases, and applications.

Management Response: The Department concurs with this recommendation. The Department will develop a corrective action plan by December 31, 2019, to address the recommendation.

OIG Recommendation 2.7: Ensure that all websites and portals hosting personally identifiable information are configured not to display clear text.

Management Response: The Department does not concur with this recommendation. The risk was accepted due to business requirements. The risk acceptance and associated details were provided to the OIG. FSA continues to research viable alternative approaches and will move to fix this once a suitable option is found. In accordance with the Department's risk management practices, the Department will periodically review the business requirements and conditions for risk acceptance.

OIG Recommendation 2.8: Eliminate the use of Social Security numbers as an authentication element when logging into FSA websites by requiring the user to create a unique identifier for account authentication. (Repeat Recommendation)

Management Response: The Department does not concur with this recommendation. The risk was accepted due to business requirements. The risk acceptance and associated details were provided to the OIG. FSA continues to research viable alternative approaches and will move to fix this once a suitable option is found. In accordance with the Department's risk management practices, the Department will periodically review the business requirements and conditions for risk acceptance.

OIG Recommendation 2.9: Immediately correct or mitigate the vulnerabilities identified during the security assessment.

Management Response: The Department concurs with this recommendation. The Department and FSA will develop a corrective action plan by December 31, 2019, to address the recommendation.

REPORTING METRIC DOMAIN No. 3: IDENTITY AND ACCESS MANAGEMENT

The OIG recommends that the Deputy Secretary and Chief Operating Officer require OCIO and FSA to:

OIG Recommendation 3.1: Incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Identity and Access Management program.

Management Response: The Department concurs with this recommendation. The Department expects to complete its corrective action and to be able to close the FY 2018 corrective action associated with this recommendation by September 30, 2021.

OIG Recommendation 3.2: Ensure that terminated individuals' network access is removed timely.

Management Response: The Department concurs with this recommendation. A similar recommendation was issued during the FY 2018 FISMA Audit, and the Department updated account management procedures to address the recommendation. Evidence of this remediation was provided to the IG of this action for their review.

OIG Recommendation 3.3: Ensure that access agreements for users accessing Department and FSA systems are documented and maintained. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. The Department will develop a corrective action plan by December 31, 2019, to address the recommendation.

OIG Recommendation 3.4: Consistently document position risk designations for background investigations.

Management Response: The Department concurs with this recommendation. The Department will develop a corrective action plan by December 31, 2019, to address the recommendation.

The OIG recommends that the Deputy Secretary require OCIO to:

OIG Recommendation 3.5: Fully implement the Department's ICAM strategy to ensure that the Department meets full Federal Government implementation of ICAM. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. The Department expects to take the corrective action and to be able to close the FY 2018 corrective action associated with this recommendation by December 31, 2020.

OIG Recommendation 3.6: Ensure that the network access control solution is fully implemented to ensure identification and authentication of devices connected to the network.

Management Response: The Department concurs with this recommendation. The Department expects to complete its corrective action and to be able to close the FY 2018 corrective action associated with this recommendation by October 31, 2019.

OIG Recommendation 3.7: Validate the inactivity settings to ensure sessions are timing out after 30 minutes of inactivity.

Management Response: The Department concurs with this recommendation. As discussed during the entrance conference for this audit, the Department's core infrastructure was transitioned to a new service provider. This transition occurred during the OIG's fieldwork, and the OIG may have tested during this transition period. The Department will develop a corrective action plan by December 31, 2019, to address the recommendation.

The OIG recommends that the Chief Operating Officer require FSA to:

OIG Recommendation 3.8: Fully implement the process for identifying, managing, and tracking activity of privileged user accounts.

Management Response: The Department concurs with this recommendation. The Department resolved the FY 2018 corrective action associated with this recommendation by making a change to account management procedures. Evidence of this remediation was provided to the IG for their review.

OIG Recommendation 3.9: Enforce a two-factor authentication configuration for all user connections to systems and applications.

Management Response: The Department concurs with this recommendation. The Department will develop a corrective action plan by December 31, 2019, to address the recommendation.

OIG Recommendation 3.10: Create corrective action plans to remedy database vulnerabilities for all database vulnerabilities identified.

Management Response: The Department concurs with this recommendation. The Department will develop a corrective action plan by December 31, 2019, to address the recommendation.

OIG Recommendation 3.11: System owners configure all websites to display warning banners when users log-in to Departmental resources and ensure that banners include approved warning language by October 31, 2019.

Management Response: The Department concurs with this recommendation. The Department expects to take the corrective action and to be able to close the FY 2018 corrective action associated with this recommendation by October 31, 2019.

REPORTING METRIC DOMAIN No. 4: DATA PROTECTION AND PRIVACY

The OIG recommends that the Deputy Secretary and the Chief Operating Officer require OCIO and FSA to:

OIG Recommendation 4.1: Incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Data Protection and Privacy program.

Management Response: The Department concurs with this recommendation. The Department expects to take the corrective action and to be able to close the FY 2018 corrective action associated with this recommendation by September 30, 2021.

The OIG recommends that the Deputy Secretary require OCIO to:

OIG Recommendation 4.2: Ensure that Privacy Impact Assessments are reviewed every two years.

Management Response: The Department concurs with this recommendation. The Department expects to take the corrective action and to be able to close the FY 2018 corrective action associated with this recommendation by November 29, 2019.

REPORTING METRIC DOMAIN No. 5: SECURITY TRAINING

The OIG recommends that the Deputy Secretary require OCIO to:

OIG Recommendation 5.1: Incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Security Training program.

Management Response: The Department concurs with this recommendation. The Department expects to take the corrective action and to be able to close the FY 2018 corrective action associated with this recommendation by September 30, 2021.

OIG Recommendation 5.2: Ensure that all new users complete the mandatory training requirements before being granted access to Departmental systems.

Management Response: The Department concurs with this recommendation. A similar recommendation was issued during the FY 2018 FISMA Audit, and the Department updated account creation procedures to address the recommendation. Evidence of this remediation was provided to the IG for their review.

The OIG recommends that the Deputy Secretary and the Chief Operating Officer require OCIO and FSA to:

OIG Recommendation 5.3: Ensure that the process for ensuring completion of role-based training is fully implemented.

Management Response: The Department concurs with this recommendation. The Department will develop a corrective action plan by December 31, 2019, to address the recommendation.

REPORTING METRIC DOMAIN No. 6: INFORMATION SECURITY CONTINUOUS MONITORING [ISCM]

The OIG recommends that the Deputy Secretary and the Chief Operating Officer require OCIO and FSA to:

OIG Recommendation 6.1: Incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the ISCM program.

Management Response: The Department concurs with this recommendation. The Department expects to take the corrective action and to be able to close the FY 2018 corrective action associated with this recommendation by September 30, 2021.

The OIG recommends that the Deputy Secretary require OCIO:

OIG Recommendation 6.2: Automate its capabilities for monitoring the security controls effectiveness and overall implementation of the ISCM Roadmap. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. The Department expects to take the corrective action and to be able to close the FY 2018 corrective action associated with this recommendation by October 30, 2020.

OIG Recommendation 6.3: Ensure the completion of Phases 1 and 2 of the CDM program. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. The Department expects to take the corrective action and to be able to close the FY 2018 corrective action associated with this recommendation by January 29, 2021.

OIG Recommendation 6.4: Implement a process that ensures data reported on the Cybersecurity Framework Risk Scorecard is accurate.

Management Response: The Department concurs with this recommendation. The Department will develop a corrective action plan by December 31, 2019, to address the recommendation.

REPORTING METRIC DOMAIN No.7: INCIDENT RESPONSE

The OIG recommends that the Deputy Secretary require OCIO to:

Recommendation 7.1: Incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Incident Response program.

Management Response: The Department concurs with this recommendation. The Department expects to close the FY 2018 corrective action associated with this recommendation by September 30, 2021.

Recommendation 7.2: Ensure that incidents are consistently submitted to the OIG within the required timeframe.

Management Response: The Department partially concurs with this recommendation. Per the discussions with the OIG after the FY 2018 FISMA audit, the Department updated the Computer Crime Incident Reporting standard to clarify that incident reporting to the Technology Crimes Division (TCD) should be focused on incidents with criminal intent.

The OCIO does have a concern that over reporting of incidents that do not show criminal intent could hinder TCD's ability to conduct investigation in a timely manner. However, to maintain transparency with the OIG and TCD, and to provide situational awareness of all incident-related information, members of the TCD were given accounts (access) to the Department's security operations incident management system. This access provides members of the TCD the ability to review all Department incidents at their discretion. If an incident is potentially criminal in nature, the Department's Security Operation Center will follow the documented reporting procedures. Nevertheless, the Department will develop a corrective action plan by December 31, 2019, to address the recommendation.

Recommendation 7.3: Ensure that data loss prevention technologies work as intended for the blocking of sensitive information transmission.

Management Response: The Department concurs with this recommendation. As noted in corrective actions for the FY 2018 FISMA Audit, the Department is currently working to ensure the new Data Loss Prevention (DLP) solutions deployed as part of the migration to a new service provider are properly safeguarding the Department's Personally Identifiable Information (PII). The Department expects to close the FY 2018 corrective action associated with this recommendation by February 28, 2020.

REPORTING METRIC DOMAIN No.8: CONTINGENCY PLANNING

The OIG recommends that the Chief Operating Officer require FSA to:

Recommendation 8.1: Incorporate additional measures to, at a minimum, achieve Level 4 Managed and Measurable status of the Contingency Planning program.

Management Response: The Department concurs with this recommendation. The Department expects to take the corrective action and to be able to close the FY 2018 corrective action associated with this recommendation by September 30, 2021.

Recommendation 8.2: Ensure that contingency plans, and other artifacts impacting contingency plans, are documented and updated in a consistent and timely manner.

Management Response: The Department concurs with this recommendation. The Department will develop a corrective action plan by December 31, 2019, 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 Officer, Jason Gray at (202) 245-6252.

cc: Jason Gray, Chief Information Officer, Office of the Chief Information Officer Ann Kim, Deputy Chief Information Officer, Office of the Chief Information Officer
Wanda Broadus, Acting 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