The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report For Fiscal Year 2017

FINAL AUDIT REPORT

ED-OIG/A11R0001
October 2017

Our mission is to promote the efficiency, effectiveness, and integrity of the Department's programs and operations.

U.S Department of Education
Office of Inspector General
Information Technology Audit Division
Washington, DC

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. Determinations of corrective action to be taken will be made by the appropriate Department of Education officials.

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.

Abbreviations and Acronyms Used in this Report

BIA	Business Impact Assessment
CDM	Continuous Diagnostics and Mitigation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CSAM	Cyber Security Assessment and Management
Department	U.S. Department of Education
DHS	Department of Homeland Security
EARB	Enterprise Architecture Review Board
EDSOC	Education Security Operations Center
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
ISA	Interconnection Security Agreement
ISCM	Information Security Continuous Monitoring
IT	Information Technology
NTT	NTT DATA Services
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
POA&M	Plan of Action and Milestones
SP	Special Publication
TIC	Trusted Internet Connection
TLS	Transport Layer Security
US-CERT	United States Computer Emergency Readiness Team

October 31, 2017

Memorandum

TO: Joseph C. Conaty
Delegated the Duties and Functions
of the Deputy Secretary

Wayne Johnson
Chief Operating Officer

FROM: Charles E. Coe, Jr.
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 2017
Control Number ED-OIG/A11R0001

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 2017. 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
Keith Wilson, Chief Information Officer, Federal Student Aid
Leslie Willoughby, Deputy Chief Information Officer, Federal Student Aid
Daniel Galik, 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
Charles Laster, Post Audit Group, Office of the Chief Financial Officer
L'Wanda Rosemond, AARTS Administrator, Office of Inspector General

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report constitutes the Office of Inspector General's independent evaluation of the U.S. Department of Education's (Department) information technology security program and practices, as required by the Federal Information Security Modernization Act of 2014 (FISMA). Our report is based on, and incorporates, the Fiscal Year (FY) 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics V1.0 (issued April 17, 2017) (FY 2017 IG FISMA Metrics) prepared by the Council of the Inspectors General on Integrity and Efficiency, the Office of Management and Budget, and the U.S. Department of Homeland Security, in consultation with the Federal Chief Information Officer Council.

What Was Our Objective?

Our objective was to determine whether the Department's and Federal Student Aid's (FSA) overall information technology security programs and practices were effective as they relate to Federal information security requirements. The FY 2017 IG FISMA Metrics are grouped into seven metric domains and organized around the five Cybersecurity Framework Security Functions (security functions) outlined in the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity:

- Identify security function (one metric domain—Risk Management);
- Protect security function (three metric domains—Configuration Management, Identity and Access Management, 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).

Under the FY 2017 IG FISMA Metrics, inspectors general assess the effectiveness of each security function using maturity level scoring.[1] The scoring distribution is based on five maturity levels outlined in the FY 2017 IG FISMA Metrics: (1) Ad-hoc, (2) Defined, (3) Consistently Implemented, (4) Managed and Measurable, and (5) Optimized. 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.

To meet the objective, we conducted audit work in the seven metric domains. We assessed the effectiveness of security controls based on the extent to which the controls were implemented

[1] The maturity model was prepared in coordination with the Office of Management and Budget and the Department of Homeland Security.

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.[2]

What We Reviewed

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 2017 FISMA Metrics. We report our results on each of these metric domains to the Office of Management and Budget as required; see Enclosure 1. Based on our work on these metric domains, we scored effectiveness against the maturity level reached within each of the five security functions.

Our audit work included the following testing procedures: (1) system-level testing for the Configuration Management, Risk Management, and Contingency Planning metric domains; (2) vulnerability assessments of systems, applications, and infrastructure; (3) verification of training evidence; (4) testing of remote access control settings; and (5) observation of Education Department Utility for Communications, Applications, and Technology Environment's comprehensive disaster recovery exercise.

During the FY 2016 FISMA audit, we found that the Department and FSA were not generally effective in three security functions (Protect, Detect, and Respond), but were generally effective in two security functions—Identify and Recover.

What We Found

As guided by the maturity model used in the FY 2017 IG FISMA Metrics, we found the Department and FSA were not effective in all five security functions—Identify, Protect, Detect, Respond, and Recover. We also identified findings in all seven metric domains: (1) Risk Management, (2) Configuration Management, (3) Identity and Access Management, (4) Security Training, (5) Information Security Continuous Monitoring, (6) Incident Response, and (7) Contingency Planning. At the metric domains level, we determined that the Department's and FSA's programs were consistent with the maturity level of Defined for Configuration Management, Identity and Access Management, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning. We determined the programs were consistent with the maturity level of Consistently Implemented for Risk Management.

The FY 2017 maturity model was more comprehensive and attributes were assessed differently than the previous year's maturity model indicator scoring. As a result, certain functions were assessed at a lower level. Despite the lower overall scoring due to changes in the maturity model, we found several areas of improvement from FY 2016. Specifically, in FY 2017, we found that the Department and FSA have made improvements in developing and strengthening their security programs. We found the Department and FSA have developed their risk management programs by establishing workshops and forums to inform stakeholders on risk

[2] 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."

management issues. The Department and FSA have made progress in defining and communicating responsibilities of configuration management to stakeholders and began performing an assessment of skills, knowledge, and resources to effectively implement a configuration management program. In March 2017, in response to a FY 2016 FISMA audit finding, the Office of the Chief Information Officer developed a strategy to replace current token access with personal identity verification cards for remote users. Also, the Department uses performance metrics and lessons learned in collaboration with communicating with its stakeholders as a way to determine whether the Information Security Continuous Monitoring program is fully integrated. In addition, to address the effectiveness of the incident response program, both the Department's and FSA's Security Operations Centers participated in tabletop exercises that provided stakeholders an opportunity to walk through the incident response process and procedures using actual incident scenarios and testing of breach responsiveness.

Although the Department and FSA made progress in strengthening their information security programs, we found weaknesses in the Department's and FSA's information systems, and those systems continued to be vulnerable to security threats.

For Risk Management, we found that improvements are needed in (1) updating inventory guidance, (2) ensuring that security control compliance and access language are included in contracts, and (3) maintaining a complete website inventory.

For Configuration Management, we found that the Department (1) was not using appropriate application connection protocols; (2) was unable to protect against unauthorized devices connecting to its network; (3) used unsupported operating systems, databases, and applications in its production environment; (4) had not configured websites to encrypt data transmission; (5) had not adequately protected personally identifiable information; and (6) did not define common secure configurations.

For Identity and Access Management, we found that the Department and FSA can strengthen their controls in the areas of (1) background investigations being completed before granting system access; (2) managing external privileged accounts; (3) Identity, Credential, and Access Management enterprise roadmap implementation plans; (4) consistently implementing the Identity, Credential, and Access Management strategy; (5) implementing the network access control solution; and (6) displaying system warning banners.

For Security Training, we found that contractors were able to obtain access to Departmental resources before fulfilling their training requirements.

For its Information Security Continuous Monitoring program, we found that the Department can strengthen its controls in the areas of (1) security control monitoring, (2) developing and identifying roles and responsibilities, and (3) fully implementing its continuous diagnostics and mitigation program.

For its Incident Response program, we found that the Department can strengthen its controls in the areas of (1) updating current guidance, (2) training key personnel, (3) timely reporting incidents, and (4) maintaining current interconnection security agreements.

For its Contingency Planning program, we found that the Department can strengthen its controls regarding contingency planning in the areas of (1) enterprise skill assessment; (2) documenting contingency plans, business impact assessments, and contingency plan testing; and (3) contingency plan completeness.

Our answers to the questions in the FY 2017 IG FISMA Metrics template, which will become the CyberScope report, are shown in Enclosure 1.

What We Recommend

This report contains seven findings, two of which are repeat findings from previous FISMA audit reports. We make 37 recommendations (4 of which are repeat recommendations) to assist the Department and FSA with increasing the effectiveness of their information security programs so that they 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. During our FY 2016 FISMA audit, we made 15 recommendations to the Department and FSA to address the 11 findings that we identified. As of October 2017, the Department and FSA reported that they have completed corrective actions for 10 of the 15 recommendations. However, despite their reporting completed corrective actions, we continue to identify repeat findings and recommendations in both the Information Security Continuous Monitoring and Incident Response metric domains. Although the Department and FSA may have taken action on specific findings, systemic issues persist in these metric domains on an enterprise level. The Department and FSA anticipate completing corrective action for all FY 2016 recommendations this fiscal year, with many scheduled for completion by the end of 2017.

The Department concurred with 31 of our 37 recommendations, partially concurred with 5 recommendations (2.4, 2.5, 3.6, 6.2, and 6.5) and did not concur with recommendation 1.2. We summarized and responded to specific comments in the "Audit Results" section of the report. The OIG considered the Department's comments and although we did not revise our findings, as a result of subsequent support provided by the Department, we removed 2 of the 37 recommendations (6.2 and 6.5).

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 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 (CIO) 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, the Federal Information Security Modernization Act of 2014 (FISMA), Public Law 113-283, 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.

In addition, FISMA revised the Federal Information Security Management Act of 2002 requirement for Offices of Inspectors General (OIG) to annually assess agency "compliance" with information security policies, procedures, standards, and guidelines. FISMA now requires OIGs to assess the "effectiveness" of the agency's information security program. It also codified certain information security requirements related to continuous monitoring that OMB had previously established. 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 (CIGIE), OMB, and DHS developed the Fiscal Year (FY) 2017 Inspector General FISMA Reporting Metrics V1.0, April 26, 2016 (FY 2017 FISMA Metrics), in consultation with the Federal Chief Information Officer Council. The FY 2017 FISMA Metrics are organized around the five information Cybersecurity Framework security functions (security functions) outlined in the NIST's "Framework for Improving Critical Infrastructure Cybersecurity," as shown in Table 1. [3]

Table 1. Aligning the Security Functions to the FY 2017 IG FISMA Metric Domains

Security Functions	FY 2017 IG Metric Domains
Identify	Risk Management
Protect	Configuration Management, Identity and Access Management, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

For FY 2015, CIGIE, in coordination with DHS, OMB, NIST, and other key stakeholders, established the maturity model for information security continuous monitoring (ISCM). The maturity model is designed to provide a perspective on the overall status of information security within an agency, as well as across agencies. In FY 2016, this effort continued by establishing an Incident Response maturity model, with plans to extend the maturity model to other security functions for OIGs to use in their FY 2017 FISMA reviews. In FY 2017, not only were the Identify, Protect, and Recover security functions transitioned into full maturity models, but the

[3] NIST's Framework for Improving Critical Infrastructure Cybersecurity defines the security functions as follows: (1) Identify—develops the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities; (2) Protect—develops and implements the appropriate safeguards to ensure delivery of critical infrastructure services; (3) Detect—develops and implements the appropriate activities to identify the occurrence of a cybersecurity event; (4) Respond—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; and (5) Recover—develops and implements the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

maturity models were reorganized to be more intuitive and in line with the CIO FISMA reporting metrics. This alignment with the Cybersecurity Framework helps promote consistent and comparable metrics and criteria in the CIO and IG metrics processes, while providing agencies with a meaningful independent assessment of effectiveness of their information security program.

The inspectors general are required by FISMA and the FY 2017 IG FISMA Metrics 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 2 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]

Table 2. Level of Maturity and Description

Maturity Level	Maturity Level Description
Level 1: Ad-hoc	Policies, procedures, and strategy are not formalized; 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 Measureable	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 2017 IG FISMA Metrics, ratings throughout the seven domains are by simple majority. Further, IGs determine the overall agency rating and the rating for each of the Cybersecurity Framework Functions at the maturity level.

Beginning in FY 2009, OMB required Federal agencies and OIGs to submit FISMA reporting through the OMB Web portal, CyberScope (Enclosure 1).

[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 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.

Departmental Systems and Security Program Description

In September 2007, the U.S. Department of Education (Department) entered into a contract with the predecessor of NTT DATA Services (NTT), to provide and manage information technology (IT) infrastructure services to the Department under the Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) system. The contract established a contractor-owned and contractor-operated IT service model for the Department under which NTT provides the enterprise IT platform and network infrastructure to support Department employees in meeting the Department's mission. The contract was awarded as a 10-year, performance-based, indefinite-delivery, indefinite-quantity contract with fixed unit prices and was due to expire in November 2017. Under this contract, NTT owns all of the IT hardware and operating systems, including wide-area and local-area network devices, network servers, routers, switches, external firewalls, voice mail, and the Department's laptops and workstations. NTT also provides help desk services and all personal computer services. NTT also managed the Department's Virtual Data Center, which was located at the contractor's facility in Plano, Texas. The Virtual Data Center is a general support system into which Federal Student Aid (FSA) consolidated many of its student financial aid program systems to improve interoperability and reduce costs. It serves as the hosting facility for FSA systems that process student financial aid applications, provide schools and lenders with eligibility determinations, and support payments from and repayment to lenders. It consists of a network infrastructure, servers, and the corresponding operating systems. Many of the financial aid applications that are hosted at Virtual Data Center are operated by other contractors. This contract expired in August 2016. NTT continued to manage the Virtual Data Center until transition to a new contractor was completed in the summer of 2017. We discuss the status of the contract recompete and transition for both computing environments in the "Other Matters" section of this report. The Department's total spending for IT investments for the FY 2017 was estimated at about $700 million.

Through the Office of the Chief Information Officer (OCIO), the Department monitors and evaluates the contractor-provided IT services through a service-level agreement framework and develops and maintains common business solutions that are required by multiple program offices. OCIO advises and assists the Secretary and other senior officials to ensure that the Department acquires and manages IT resources in a manner that is consistent with the requirements of the Clinger-Cohen Act of 1996,[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 IT investments, and leading change to improve the efficiency and effectiveness of the Department's operations. In addition to OCIO, FSA has its own CIO, 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 CIO core business functions

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

include the (1) Application Development Group, (2) Enterprise IT Management Group, and (3) Enterprise IT Services Group.

Fiscal Year 2016 FISMA Audit Results

During last year's FISMA audit, we identified 11 findings and provided 15 recommendations that addressed the conditions noted in the report. The Department concurred with 14 recommendations, partially concurred with 1, and provided corrective action plans on how it would address the recommendations. In general, our findings identified:

- outdated policies and procedures;
- the use of unsecure application protocols;
- control weaknesses in web applications, network infrastructure, and database management;
- insufficient of enforcement of personal identification verification for nonprivileged users;
- 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 updating policies and procedures, developing new guidance, instituting secure connection protocols for its systems, completing network access control deployment, creating Plans of Action and Milestones (POA&M) for all vulnerabilities identified in the FY 2016 report, updating security documentation as needed, improving communication and escalation of identified issues with OIG, and developing a cybersecurity workforce strategy. As of October 2017, the Department and FSA reported that they had completed corrective actions for 10 of the 15 recommendations. The Department and FSA anticipate completing corrective action for all recommendations this fiscal year, with many scheduled for completion by the end of 2017.

AUDIT RESULTS

Based on the requirements specified in FISMA and the FY 2017 IG FISMA Metrics, our audit focused on reviewing the five security functions and associated metric domains: Identify (Risk Management), Protect (Configuration Management, Identity and Access Management, and Security Training), Detect (ISCM), Respond (Incident Response), and Recover (Contingency Planning). The FY 2017 maturity model was more comprehensive and attributes were assessed differently than the previous year's maturity model indicator scoring. As a result, certain functions were assessed at a lower level, and we found the Department and FSA were not effective in all five security functions—Identify, Protect, Detect, Respond, and Recover.

We identified findings in Risk Management, Configuration Management, Identity and Access Management, Security Training, ISCM, Incident Response, and Contingency Planning metric domains. Our findings in these metric domains included repeat findings from the following OIG reports issued from FYs 2011 through 2016:

- "The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2011," (ED-OIG/A11L0003) October 2011;
- "The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2012," (ED-OIG/A11M0003) November 2012;
- "The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013," (ED-OIG/A11N0001) November 2013;
- "The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014," (ED-OIG/A11O0001) September 2014;
- "The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2015," (ED-OIG/A11P0001) November 2015; and
- "The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2016," (ED-OIG/A11Q001) November 2016.

SECURITY FUNCTION 1—IDENTIFY

The "Identify" security function comprises the Risk Management metric domain. Based on our evaluation of the Department's Risk Management program, we determined that the Identify security function was consistent with the Consistently Implemented level of the maturity model, which is categorized as being not effective. Of the twelve metrics for this domain, we found the Department and FSA to be at the Consistently Implemented level for 8 metrics, the Defined level for 3 metrics, and the Ad Hoc level for one metric. We found the Department and FSA (1) established policies and procedures consistent with NIST standards, (2) relied on a Department-wide Risk Management Framework, (3) established a risk methodology to assess its systems on an ongoing/continuous basis, (4) established an inventory of relevant documentation needed to assess system risk, (5) migrated to a new solution for its system documentation, and (6) established workshops and forums to inform stakeholders on risk management issues. Nonetheless, we noted some improvements are needed in (1) updating inventory guidance,

(2) including contract security control compliance and access language, and (3) maintaining a complete website inventory.

METRIC DOMAIN 1—RISK MANAGEMENT

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. A POA&M, also referred to as a corrective action plan, is a management tool for tracking the mitigation of cybersecurity program and system-level findings and weaknesses. The purpose of a POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.[7]

We determined that the Department's and FSA's Risk Management program was consistent with the Consistently Implemented level of the maturity model, which is categorized as being not effective. The Department and FSA have consistently implemented its risk management policies, procedures, and strategies at the enterprise, business process, and information system levels, and use its risk profile to facilitate a determination on the aggregate level and types of risk that management is willing to assume. Moreover, both the Department and FSA consistently capture and share lessons learned on the effectiveness of risk management processes and activities in need of program improvements with its respective shareholders. However, while the Department has made several improvements to its risk management program, its practices in several areas still do not meet the Managed and Measurable threshold under the metrics required to be considered effective. To meet the Managed and Measurable level, the Department would need to achieve this level in at least 7 of the 12 metric areas. For example, the Department would need to ensure that the hardware assets connected to the network comply with the monitoring processes defined within Department's ISCM strategy.

In FY 2016, based on the maturity model indicator scoring, we determined that the Department's and FSA's "Identify" security function (which comprised Risk Management and Contractor Systems) was scored at Level 5: Optimized, which was categorized as effective. Specifically, the Department and FSA had developed a comprehensive governance structure and organization-wide risk management strategy and program that included comprehensive agency policies and procedures consistent with OMB policy and applicable NIST guidelines. Because the FY 2017 maturity model was more comprehensive and attributes were assessed differently than the previous year's maturity model indicator scoring, the Department was assessed at a lower level.

The Department established a risk management process that includes policies and procedures and an enterprise strategy for its business process and information systems. It uses its risk profile to facilitate a determination on the aggregate level and types of risk that management is willing to assume and consistently captures and shares lessons learned on the effectiveness of risk management processes and activities to update the program.

[7] In prior years' reporting, the POA&M and Contractor Systems areas were reported as separate metric domains. However, for FY 2017 FISMA reporting, POA&M and Contractor Systems metric questions are incorporated into the Risk Management metric domain.

The Department defined an information security architecture that is integrated into and supports its enterprise architecture and provides a structured methodology for managing risk. In addition, it defined a process to conduct a security architecture review for newly acquired hardware and software before introducing systems into its development environment. According to the OCIO-01, "Information Assurance Cybersecurity Policy," the OCIO, in coordination with the principal offices, is required to establish and maintain an architecture that includes security for both the Department's network components and connected information systems (i.e., the "enterprise"). Principal offices are required to obtain the approval of the Enterprise Architecture Review Board (EARB) before the development or acquisition of an information system. The Department's information systems are required to have baseline security requirements in compliance with this policy and all Federal cybersecurity authorities and regulations.

We determined that the Department developed the capability to build and maintain a system inventory that included all FISMA reportable systems, cloud systems, and contractor systems, and determined that it uses standard data elements/taxonomy to develop and maintain an inventory of hardware assets with the exceptions of the finding listed below.

The Department also implemented an automated solution across the enterprise that provides a centralized, enterprise-wide view of risks, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. We determined that the Department and FSA have fully migrated to the Cyber Security Assessment and Management (CSAM) system, which serves as their repository for all system information such as security authorization data, POA&Ms, and risk acceptance forms.

The Department developed the Information Assurance Services 02, "System Inventory Methodology and Guidance," for developing, managing and maintaining an inventory of IT systems that satisfied FISMA system reporting requirements. It also provides detailed guidance for managing the Department's FISMA system inventory within the CSAM tool. The Department also developed the Information Assurance Services 03, "System Categorization Guidance," to provide a detailed direction for conducting, documenting, and maintaining security categorization levels across the Department. The guidance is designed to facilitate the application of appropriate levels of information security according to a range of levels of impact or consequences that might result from the unauthorized disclosure, modification, or use of the information or information system.

Furthermore, as part of the Department-wide Risk Management Framework, the Department developed assessments to identify program's knowledge, skills, abilities, and resource gaps. These included results from assessment activities such as (1) the DHS Continuous Diagnostics and Mitigation (CDM) Governance Support Plan (People and Organizational Assessment subsection), (2) the Department's Cybersecurity Workforce Baseline Certification Assessment, and (3) CDM Phase 1 Implementation Readiness Review. We also noted that roles and responsibilities have been expanded in the more recent policies that were produced in FY 2017.

The Department established a risk assessment process that incorporates NIST Special Publication (SP) 800-30, "Guide for Conducting Risk Assessments." Risk assessments (formal or informal) are conducted at various steps in the Risk Management Framework that includes (1) information system categorization, (2) security control selection, (3) security control

implementation, (4) security control assessment, (5) information system authorization, and (6) security control monitoring (continuous monitoring). System risk assessments are performed and appropriate security controls are implemented on a consistent basis. The Department uses the common vulnerability scoring system, or a similar approach, to communicate the characteristics and severity of software vulnerabilities.

As part of the Department's risk assessment process, assessors are required to share identified risks with all levels of management. The resulting risk rating is conveyed to the Authorizing Official who approves the system security plan, authorizes the system to operate, and directs corrective actions to mitigate risk to an acceptable level. The Authorizing Official provides feedback to the system owner on which vulnerabilities (e.g., noncompliant security controls) must be corrected and the acceptable timeframe for corrective actions.

The Department communicated information about risks in a timely and consistent manner to all internal and external stakeholders with a need to know. Furthermore, the organization actively shares information with partners to ensure that accurate, current information is being distributed and consumed.

We found that the Department had established forums and workshops to train and educate stakeholders on risk management issues. We attended a Quarterly Cybersecurity Risk Management Workshop that addressed issues such as (1) cybersecurity policy and guidance updates, (2) outstanding POA&Ms, and (3) ensuring compliance for secure connections for websites and services. We also attended the Cybersecurity Risk Management Forum where Department officials discussed issues regarding governance, risk, and compliance. Issues discussed included POA&M aging and status, and NIST SP 800-53, Revision 4, "Security and Privacy of Controls for Federal Information Systems and Organizations," and control family classification.

OCIO manages the Department's IT Investment Management process to ensure consistency with all applicable legislation, as well as the Department's enterprise architecture, information management, information assurance, and related standards and processes. The IT Inventory Management process is intended to ensure that IT investments (1) support and are aligned with the Department's business objectives and Strategic Plan; (2) comply with all relevant statutes, Federal regulations, and Departmental policies; (3) do not duplicate other investments; and (4) are carefully selected and managed in a way that demonstrates careful decision making, with the greatest possible partnership and resource sharing both within the Department and other agencies.

The Department established a POA&M process in accordance with the Department's policies and procedures to mitigate security weaknesses. We verified that the Department uses the CSAM repository to store and track its POA&Ms and is looking to automate portions of the process to assist in reducing the number of outstanding POA&Ms. We performed a review of 987 outstanding POA&Ms and found that (1) 849 of 987 (86 percent) were over 90 days; (2) 61 of 987 (6 percent) were over 200 days; and (3) there were no POA&Ms greater than one year.

Based on our evaluation, we identified the following areas of improvement for this metric area.

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

Of the 12 metrics for the Risk Management Domain, we found the Department and FSA to be at the Consistently Implemented level for 8 metrics, the Defined level for 3 metrics, and the Ad Hoc level for 1 metric. We found that the Department should strengthen its controls regarding risk management in the areas of (1) updating inventory guidance, (2) ensuring Federal security control compliance and access to contractor and subcontractor systems, and (3) maintaining a complete website inventory.

Inventory Guidance Was Not Current

We found that the Department continues to rely on its "Information Technology Security General Support Systems and Major Applications Inventory Guidance, Version 1.0," dated March 2009. We have cited this outdated guidance in our FISMA reports since FY 2012. This guidance is designed to lead to the successful completion of the Data Sensitivity Worksheet for each information system and to result in an accurate inventory of the Department's system. However, this guidance has not been updated since March 2009, and therefore it does not incorporate all current NIST and OMB guidance regarding systems inventory.

Contracts Did Not Include Security Control Compliance and Access Language

The Department did not ensure that all required security language, including a provision allowing access to contractors and their subcontractors, was included in contracts relating to contractor systems and services. We reviewed the contracts for the 10 externally hosted systems that were judgmentally selected for this year's audit, as well as a contract for a system that was recently awarded to determine whether the 11 contracts contained, at a minimum, security language for ensuring that the systems were in compliance with security control requirements.[8] Our review determined that three system contracts did not contain language requiring contractors to comply with Federal security controls. OCIO informed us that although the Department developed standard security contract language for its contracts, they are reviewing and reevaluating current contract language for consistency across principal offices and contracts. The expectation is that all requests for proposal are reviewed before going to the contracting office for review to ensure security language is included in the contract.

Acquisition Alert 2016-07, "Class Deviation to Implement Policy Regarding Access to Contractor Information Systems," issued by the Office of the Chief Financial Officer on August 9, 2016, obligates contracting officers and contract specialists to include certain provisions and/or clauses to ensure compliance with Departmental policy regarding access to contractor or subcontractor information systems. Of the 11 contracts we reviewed, 4 were issued on or after August 9, 2016, and were subject to Acquisition Alert 2016-07. Of these four contracts, none included the mandated clause "Access to Contractor and Subcontractor Information Systems." For the other seven contracts that were issued before Acquisition Alert 2016-07, we found that four of the contracts did not contain provisions and/or relevant clauses that would allow Departmental access to contractors or subcontractor information systems. The lack of communication between the contractors and contracting officer representatives at the

[8] Since the current EDUCATE system was being replaced by sectional contracts, we selected a sectional component contract, Portfolio of Integrated Value-Oriented Technologies-M, that was already awarded.

Department regarding inclusion of relevant contract provisions, as well as limited monitoring of contractual obligations, further contributed to this condition. Without an access clause included in its service contracts, the Department cannot ensure that it will have access to contractor systems enabling it to perform necessary quality assurance, audit, and investigative functions required by Federal guidance**.**

The Department Did Not Maintain an Updated Systems Inventory for Active Websites

We found the Department's system inventory does not accurately reflect all active websites providing services for the Department. Specifically, when we compared the list that was provided during the FY FISMA 2016 audit to the current inventory, that list included an additional 61 active/online websites that were not included in the FY 2017 inventory. We verified that the additional 61 websites were still operational and accessible to users. Based on the information provided, we determined that there is no single source to provide a complete list of websites providing services for the Department. Instead, lists are provided by different sources and no centralized location is used to corroborate and maintain an accurate list.

NIST SP 800-53, Revision 4, CM-8 – Information System Component Inventory, states that organizations should develop and document an inventory of information system components that (1) accurately reflects the current information system, (2) includes all components within the authorization boundary of the information system, and (3) is at the level of granularity deemed necessary for tracking and reporting. It further states that the organization should (1) update the inventory of information system components as an integral part of component installations, removals, and information system updates; and (2) provide a centralized repository for the inventory of information system components. Although the Department Handbook OCIO-01 requires each principal office to maintain a current inventory of systems, hardware and software assets, and information (data) under its control throughout the respective system development life cycles, the Department lacked a centralized tracking process to ensure that its inventory was complete and current. Failure to identify and maintain an updated inventory—specifically, one that accurately reflects all active websites managed by the Department—could lead to compromise and exposure of data without the Department knowing that it had occurred.

Recommendations

We recommend that the Deputy Secretary require OCIO to—

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

1.2 Ensure that "Information Technology Security General Support Systems and Major Applications Inventory Guidance, Version 1.0" is updated.

1.3 Ensure that all contracts are reviewed and reevaluated to ensure that required access and security language is included.

1.4 Establish a centralized tracking process for maintaining all active websites for the Department.

Management Comments

The Department concurred with recommendations 1.1, 1.3, and 1.4 but did not concur with recommendation 1.2. For recommendations 1.1, 1.3, and 1.4, the Department stated it will develop corrective action plans by December 1, 2017, to address the associated finding. For recommendation 1.2, the Department stated it released Information Assurance Services 02, "Systems Inventory Methodology and Guidance," and the Information Assurance Services 03, "System Categorization Guidance," that superseded the "Information Technology Security General Support Systems and Major Applications Inventory Guidance, Version 1.0."

OIG Response

The OIG will review the corrective action plans to determine whether the actions will address the finding and recommendations and, if so, will validate them during our FY 2018 FISMA audit.

Regarding recommendation 1.2, the OIG identified Information Assurance Services 02 and 03 as active guidance during the audit; however, we also found that the Information Technology Security General Support Systems and Major Applications Inventory Guidance, Version 1.0, still served as the overarching policy and had not been officially superseded. On October 28, 2017, the OIG confirmed the guidance remained on the Department's intranet website and did not see any indication that this guidance had been officially superseded. If the OIG receives confirmation that the Department has removed the guidance from its intranet site, we will consider this action to be responsive to the finding and recommendation.

SECURITY FUNCTION 2—PROTECT

The "Protect" security function comprises the Configuration Management, Identity and Access Management, and Security Training metric domains. Based on our evaluation of the three program areas, we determined that the Protect security function was consistent with the Defined level of the maturity model, which is categorized as being not effective. Strengths and areas of improvement are identified individually in each of the metric domain sections below.

In FY 2016, the Department and FSA were measured against a maturity model indicator scoring system for these three metric domains and were categorized at the Defined level for this security function due to our findings in the three metric domains. For example, in configuration management, we found (1) select policies and procedures were not current with NIST and Departmental guidance, (2) appropriate application connection protocols were not being used, and (3) the Department was unable to prevent unauthorized devices from connecting to the network. All three findings were repeat findings from our FY 2015 FISMA audit and continue to exist. Through our vulnerability assessment testing, we found that the Department's and FSA's controls over web applications, as well as the application's network infrastructure need improvement. For Identity and Access Management, we performed database management assessments that identified vulnerabilities, configuration errors, rogue installations, and access issues for databases residing in the Office of General Counsel Case and Activity Management System, Education Security Tracking and Reporting System, Personal Authentication Service,

and Common Origination and Disbursement environments. Further, we found that two-factor authentication[9] for nonprivileged users is not effectively implemented and external network connections did not use two-factor authentication—another repeat finding from the FY 2015 FISMA audit. We also found that although the Department established processes and controls to ensure an effective Security Training program, we identified an area in which the Department can improve its assessment of contractors with significant security and privacy responsibilities.

METRIC DOMAIN 2—CONFIGURATION MANAGEMENT

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

We determined that the Department's and FSA's configuration management programs were consistent with the Defined level of the maturity model. The Department and FSA have defined the roles and responsibilities at the organizational and information system levels for stakeholders involved in information system configuration management. Also, these roles and responsibilities have been communicated across the organization. The Department also developed an organization-wide configuration management plan that includes the necessary components. Furthermore, Department and FSA consistently implemented Trusted Internet Connections (TIC) approved connections and critical capabilities that were managed internally. However, while the Department has made several improvements to its Configuration Management program, its practices in several areas still do not meet the Managed and Measurable threshold under the metrics to be considered effective. To meet Managed and Measurable, the Department would need to achieve that level in at least 5 of the 8 metric areas. For example, the Department would need to employ automated mechanisms (such as application whitelisting and network management tools) to detect unauthorized hardware, software, and firmware on its network and take immediate actions to limit any security impact.

The Department has made progress in defining and communicating the responsibilities of configuration management to stakeholders and began performing an assessment of skills, knowledge, and resources to effectively implement a configuration management program and continues to work to ensure this is developed across the Department. These areas are included as part of Risk Management forums that are held throughout the year. OCIO also relies on its current workforce strategy to accomplish these assessments.

The Department's Life Cycle Management Framework provides the foundation for the implementation of standards, processes, and procedures for acquiring and developing IT solutions. It requires that configuration management plans identify the configuration items, components, and related work products that will be placed under configuration management using configuration identification, configuration control, and configuration status accounting and configuration audits. It also ensures that the plan will establish and maintain the integrity of

[9] Two-factor authentication is a security process in which the user provides two means of identification from separate categories of credentials; one is typically a physical token, such as a card, and the other is typically something memorized. This additional layer of security could help reduce the incidence of online identity theft, phishing expeditions, and other online fraud.

work products throughout the life cycle. The Department also uses the Life Cycle Management Framework policy that provides guidance on how changes are communicated to users.

The EARB is responsible for strategic decision making and communication to achieve the enterprise vision for technology at the Department level. Changes implemented on individual systems are the responsibility of the system owners. NTT manages the Department's Configuration Management Plan. The Department also relies on the system owners to include the change management plan as part of their contract.

The Department has developed configuration management plans and outlined information system configuration management policies and procedures in their overarching policies governing configuration management. As part of this process, system vulnerability scans conducted by the Department are reviewed to provide assurance that policies are being disseminated and enforced. Configuration management plans are being actively used and are submitted through the EARB process when approving systems.

As part of the Department's configuration management policy, each system is required to have its own system specific configuration management plan describing the processes for identifying and managing changes to that system. These processes are being followed when the Department performs assessments and/or independent security control assessments. Each system is required to have a Configuration Management Plan that details the system's processes that enables OCIO to gain an understanding of the system before testing the controls. If the system does not have a plan, a finding and POA&M are created and the finding is entered into CSAM.

NTT relies on its own patch management policies to remediate vulnerabilities found in the Department's systems that incorporate the guidance outlined in OCIO-01, "Information Assurance/Cybersecurity Policy."[10] Also, the Department has an independent verification and validation team that completes assessments to ensure that vulnerabilities have actually been remediated.

The Department established a vulnerability and patch management process. This process included (1) creating a system inventory; (2) monitoring for vulnerabilities, remediations, and threats; (3) prioritizing vulnerability remediation; (4) creating a remediation database; (5) testing and deploying remediations; and (6) verifying remediation. In addition, the Department established security metrics measuring a system's susceptibility to an attack, as well as mitigation response time. FSA has also its own patch management process that consisted of (1) patch notification, (2) deployment, (3) testing, (4) post-production implementation review, (5) patch validation, and (6) bimonthly patch reporting.

The Department uses security concepts to manage and maintain security baseline configurations. This included (1) configuration planning and management, (2) identifying and implementing configuration settings, (3) configuration change control, and (4) configuration monitoring. We also found that the Department established a security baseline for its systems. This included (1) Federal Desktop Core Configurations, (2) U.S. Government Configuration Baselines, and (3) Education Baseline Configurations.

[10] NTT Data Services Federal Government, Inc., provides the services for the EDUCATE contract.

The Department also established a system-hardening process for standard Windows, Linux, and UNIX operating systems. In addition, FSA established a hardening standard process for maintaining and updating hardware and software components.

The Department is an enterprise-wide TIC provider and manages two TICs (one primary and one alternate) that are shared by the Department and FSA. In FY 2015, DHS performed a TIC Capability Validation of the Department's TIC implementation and found that the Department was at 96 percent for TIC 2.0 capabilities implementation, 98 percent for external network traffic to and from the organization's networks passing through a TIC, and 100 percent of network/application interconnections to/from the organization's networks passing through a TIC. The Department informed us it had completed projects to enforce TIC requirements for multifactor authentication for administrative access to Department systems and to add redundancy to its internal Network Time Protocol capabilities. The Department stated that the completion of these projects increased its compliance with TIC 2.0 critical capabilities to 98 percent. In FY 2017, the focus has been on the establishment of TIC access points for the Department's Next Generation Data Center.

Issue 2. The Department and FSA's Configuration Management Program Needs Improvement

Of the eight metrics for the Configuration Management domain, we found the Department and FSA to be at the Defined level for six metrics, the Consistently Implemented level for one metric, and the Ad Hoc level for one metric. We found that the Department (1) was not using appropriate application connection protocol; (2) was unable to protect against unauthorized devices connecting to its network; (3) used unsupported operating systems, databases, and applications in its production environment; (4) had not configured websites to encrypt data transmission; (5) failed to adequately protect personally identifiable information; and (6) along with FSA, needs to improve its controls over web applications and servers.

The Department Was Not Using Appropriate Application Connection Protocols

During our FY 2015 and 2016 FISMA audits, we identified several authorized connections that used outdated security connection protocols. The Department concurred with the findings and introduced planned corrective actions to mitigate the known risks. However, we found that the Department continued to use the previously identified outdated secure connection protocols as a connection mechanism. Specifically, out of the 276 Department authorized active connections, 30 (11 percent) did not adhere to the mandated encryption standards of Transport Layer Security (TLS) 1.1 and above. NIST required agencies to develop migration plans to support TLS 1.2 by January 1, 2015. The Department did not restrict the use of nonsecure Secure Socket Layer version 3 connections to its network and did not take the necessary steps to ensure only recommended secure TLS connections were used.

Per the Department's policies, if the Department decides to accept the risks with identified controls weaknesses or vulnerabilities, it must complete and submit a Risk Acceptance Form. We reviewed all Risk Acceptance Forms the Department and FSA provided, and we did not find any forms that related to the use of Secure Socket Layer version 3 or TLS version 1.0 for the specific active connections. The transition from Secure Socket Layer version 3 to TLS

connection would help safeguard user information by providing a more secure connection. Despite committing to address this issue in FY 2015 and 2016, the Department has continued to use vulnerable protocols, and users could still expose systems to a number of vulnerabilities and exploits, including man-in-the-middle attacks that could jeopardize Department resources.[11]

The Department Was Unable to Prevent Unauthorized Devices From Connecting to Its Network

The Department had not implemented a solution to consistently restrict the use of unauthorized devices that connect to its network. The Department plans to use a network access control[12] solution to account for and control systems, along with peripherals on its network. We originally identified this issue in our FY 2011 FISMA audit report. Despite the Department's commitment to restrict unauthorized access on its network, the network access control solution was not effectively implemented. Our testing in June 2016 showed that the network access control solution was not able to restrict our access. In April 2017, the Department stated that the network access control solution was successfully implemented to block access to all non-Government furnished equipment. However, our testing again allowed us to gain access to a number of internal resources by connecting to the Department's network with non-Government furnished equipment. Despite the Department's assertion that the network access control solution was successfully implemented, the Department was unable to properly configure its network access control solution to restrict the availability of network resources to only endpoint devices that comply with its defined security policy.

The Department Continued to Rely on Unsupported Operating Systems, Databases, and Applications in the Production Environment

In 2015, we identified that the Department relied on a number of operating systems on the EDUCATE system that are no longer supported by their vendors. At that time, the Department was unable to provide any documentation, such as Risk Assessment Forms, to justify the use of unsupported systems, and committed to discontinue the use of these obsolete systems or develop justification for their continued use by September 2016.

During this year's audit, we found that the Department and FSA still relied on a number of operating systems, databases, and applications that were not supported by the vendors. The Department advised application owners to submit corrective action plans to upgrade the systems or submit Risk Acceptance Forms. However, it was unable to provide any documentation, such as Risk Assessment Forms, to justify the continued use of unsupported systems. Because the vendors were no longer supporting these systems, no one was addressing new vulnerabilities, leaving the Department's operating systems at unknown risk and with no alternate plan of actions.

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

[12] Network access control is a policy-enforcement mechanism designed to authenticate and authorize systems attempting to connect to a network.

Department Relied on Unsecure Web Connections

The Department did not enable the use of an encryption protocol on 151 out of the 478 websites in its inventory to protect users and their information being submitted via web portals. OMB M-15-13, "Policy to Require Secure Connections Across Federal Websites and Web Services," requires that all publically accessible Federal websites and web services provide service only through a secure connection. Further, agencies must make all existing websites and services accessible through a secure connection (HTTPS-only, with HSTS) by December 31, 2016.[13] We found that only 327 of 478 (68 percent) active websites provided by the Department enforced the secure connection protocol mandate.

Personally Identifiable Information Not Consistently Protected

The Department is not ensuring the protection of personally identifiable information—primarily Social Security number information—requested through its website by displaying information entered in clear text. Further, the Department continues to use Social Security numbers as an identifier. Specifically, we found that out of the 478 websites we reviewed, 4 websites required users to login with the use of the Social Security numbers. Additionally, none of the 4 websites were configured to mask sensitive personally identifiable information, and 1 of the 4 used Social Security number as a primary identifier. We identified a similar condition relating to using Social Security numbers as a primary identifier in our FY 2014 FISMA audit.

Websites Not Displaying Warning Banners

The Department has websites that do not display warning banners when users login to Departmental resources. The Department provided 5 separate lists of websites totaling 478 active websites. We judgmentally selected the largest list that included 252 websites and tested to see if the websites displayed a banner notifying users that they were accessing a Government system. Of the 252 sites tested, 33 (13 percent) did not display a login banner as mandated by NIST and Departmental guidance. The Department failed to configure all of its websites to ensure compliance with login banner requirements.

The Department's and FSA's Controls Over Web Applications and Servers Need Improvement

As part of our security and vulnerability testing for the FISMA FY 2017 audit, we performed web application and server vulnerability assessments for 9 of the 10 judgmentally selected systems.[14] As a result of our testing, we found that the Department and FSA should increase implementation and management of its technical security architectures supporting applications and infrastructure to restrict unauthorized access to information resources to protect it against potential application compromise. Specifically, our testing identified that although some key controls were effectively implemented (such as network segmentation, endpoint protection, and firewalls), the security architecture could use further enhancements to strengthen the

[13] 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.

[14] Refer to the "Objective, Scope, and Methodology" section of this report for a complete list of systems subject to our testing.

Department's overall security posture. For example, we identified instances of (1) SQL injection execution vulnerabilities, (2) unsecure web protocols, (3) impersonation of user sessions, (4) unprivileged access, (5) remote code execution, and (6) missing patches.

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) configuration management policies and procedures, (2) baseline configuration, (3) minimization of personally identifiable information, (4) unsupported system components, and (5) transmission confidentiality and integrity.[15] NIST SP 800-52, "Guidelines for the Selection, Configuration and Use of Transport Layer Security Implementations," states that TLS version 1.1 is required, at a minimum, to mitigate various attacks on version 1.0 of the TLS protocol. Support for TLS version 1.2 is strongly recommended and agencies are required to develop migration plans to support TLS 1.2 by January 1, 2015. NIST SP 800-46, Revision 1, "Guide to Enterprise Telework and Remote Access 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.

Relying on the outdated procedures; unsupported operating systems, databases, and applications; application connection protocols; and improper configurations of access privilege and web encryption could lead to data leakage and exposure of personally identifiable information that can compromise the Department's integrity and reputation. In addition, 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.

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 Immediately correct or mitigate the vulnerabilities identified during the vulnerability assessment.

2.3 Ensure POA&Ms are created to remedy infrastructure vulnerabilities identified in the hosting data center environments.

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

We recommend that the Deputy Secretary require OCIO to—

2.4 At a minimum, enforce TLS 1.1 or higher as the only connection for all Department connections. (Repeat Recommendation)

2.5 Discontinue the use of or develop a justification for using unsupported operating systems, databases, and applications. (Repeat Recommendation)

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

2.7 Configure all websites to display warning banners when users login to Departmental resources.

We recommend that the Chief Operating Officer require FSA to—

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

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

Management Comments

The Department concurred with recommendations 2.1 to 2.3 and, 2.6 to 2.9, and partially concurred with recommendations 2.4 and 2.5. For recommendations 2.1 to 2.3 and 2.6 to 2.9, the Department stated it will develop corrective action plans by December 1, 2017, to address the associated finding.

For recommendation 2.4, the Department stated that OCIO published the requirement to implement Transport Layer Security (TLS) version 1.1 in section *4.15.2 Policies* of the *Departmental Handbook for Information Assurance/Cybersecurity Policy (OCIO-01)*, dated January 18, 2017. As a result of the FY 2016 FISMA report and associated finding, the Department also stated it led an effort to ensure that POA&Ms and/or Risk Acceptance Forms, as appropriate, were completed for each system that was identified to have this vulnerability. The Department further stated that it will work with the OIG to validate this finding and, if required, develop a corrective action plan by December 1, 2017, to address the associated finding.

For recommendation 2.5, the Department stated that at the time of the response, OCIO has not received the background information from the OIG to validate this finding. It also stated that some software may be listed as "unsupported" by the vendor, but there may be mitigations in place that allows the continued use of the software on the network. The Department further stated that it will work with the OIG to validate this finding and, if required, develop a corrective action plan by December 1, 2017, to address the finding.

OIG Response

The OIG will review the corrective action plans to determine whether the actions will address the finding and recommendations and, if so, will validate them during our FY 2018 FISMA audit.

Regarding recommendation 2.5, the OIG will provide the background information to assist OCIO in validating the finding. Once the corrective action plan is developed, the OIG will review it to determine whether the actions will address the finding and recommendation and, if so, will validate them during our FY 2018 FISMA audit.

METRIC DOMAIN 3—IDENTITY AND ACCESS MANAGEMENT

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

We determined that the Department's and FSA's Identity and Access Management programs were consistent with the Defined level of the maturity model. The Department's and FSA's roles and responsibilities at the organizational and information system levels for stakeholders involved in Identity, Credential, and Access Management (ICAM) have been fully defined and communicated across the organization. This includes, as appropriate, developing an ICAM governance structure to align and consolidate the agency's ICAM investments, monitoring programs, and ensuring awareness and understanding. However, while the Department has made several improvements to its Identity and Access program, its practices in several areas still do not meet the Managed and Measurable threshold under the metrics to be considered effective. To meet Managed and Measurable, the Department would need to achieve that level in at least 5 of the 9 metric areas. For example, the Department would need to demonstrate that it has transitioned to its desired or "to-be" ICAM architecture and has integrated its ICAM strategy and activities with its enterprise architecture and the Federal Identity, Credentialing and Access Management segment architecture.

The Department established OCIO-01, "Information Assurance/Cybersecurity Policy," dated January 2017, which sets forth Department-level policies regarding (1) roles and responsibilities of various senior positions relating to IT security; (2) the annual review of the policy by the Department's Chief Information Security Officer; (3) access control and authentication; (4) personnel security; (5) security screening for all contractor and subcontractor employees (supplemented by OM 5-101, "Contractor Employee Personnel Security Screening"); (6) the display of system warning banners; (7) system rules of behavior; (8) network access control; (9) remote access; (10) user session timeout; and (11) management of unsupported system components on Department information systems.

The Department established Information Assurance Services 01, "Logical Access Control Guidance" in October 2016. It identifies roles and responsibilities, as well as requirements for the selection, implementation, monitoring, and enforcement of logical access controls as they

relate to Department's information systems. These requirements include (1) managing privileged user accounts, (2) using multifactor authentication (personal identification verification or token) for remote access, (3) the design and configuration of automated monitoring capabilities and control of remote access methods, (4) the design and configure with cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions, (5) session termination after 30 minutes of inactivity, (6) the display of system warning banners, and (7) system rules of behavior.

The Department issued the ICAM Enterprise Roadmap and the ICAM Implementation Plan in March 2017. The Roadmap and the Implementation Plan identify the goals and objective of the Department's ICAM programs and the targeted timeline on meeting of them.

In March 2017, OCIO developed a token replacement strategy in response to a FY 2016 FISMA OIG audit finding. The strategy was designed to replace current token access with personal identity verification cards for remote users who access the Department's network using non-Government furnished equipment but do not require physical access to Department offices.

Issue 3. The Department's and FSA's Identity and Access Management Program Needs Improvement

Of the nine metrics for the Identity and Access Management domain, we found the Department and FSA to be at the Defined level for seven metrics and the Ad Hoc level for two metrics. We found that the Department and FSA can strengthen their controls regarding identity and access management to enable them to progress to the next maturity level in the areas of (1) ensuring appropriate clearance requirements are met before granting system access, (2) managing external privileged accounts, (3) implementing the ICAM strategy, (4) implementing the network access control solution, (5) displaying system warning banners, and (6) improving controls over database management.

Access to Systems Granted Without Background Investigations

The Department and FSA did not adhere to the required Federal background investigation process for granting and monitoring access to its external users. In particular, we found contractors with privileged user access to Department and FSA systems that did not have required background investigations. This included external token users with access to EDUCATE systems, as well as foreign nationals with access to Department and FSA external systems. We also found that FSA allowed contractors to grant access to users without ensuring the applicable clearance requirements had been met. In addition, FSA failed to ensure that those employees had appropriate background investigations for the required level of access. FSA began investigating these issues in March 2017 and as of July 2017, the issues had not been resolved. By allowing users without proper clearance to access its systems and data, the Department exposes itself to the risk of providing people with the potential to do harm to the Department and the opportunity to compromise Departmental information resources. Furthermore, in addition to allowing the contractors to grant access to privileged users via personal identity verification interoperable cards, FSA lacked the ability to track and monitor the activity of those users.

FSA Did Not Manage Its External Privileged User Accounts

FSA did not have an effective process for identifying, managing, or tracking activity of privileged user accounts.[16] Specifically, we found that FSA could not account for a complete inventory of its external privileged user accounts. FSA estimated that there were about 1,600 privileged users on its systems; however, FSA was not able to validate the actual number of active accounts. Only after FSA was notified that these concerns existed did it request user activity logs of those privileged users and initiate an investigation into this issue. As of July 2017, FSA still had not completed the review of the activity logs of these privileged users.[17] Without an accurate accounting of privileged users accessing Departmental systems and data, as well as not reviewing privileged user activity, the Department has no assurance privileged user activity did not result in the compromise of its systems and/or data.

ICAM Strategy Had Not Been Finalized

We found that the Department was in the process of creating its ICAM structure during FY 2017 and is targeted to have full Federal implementation of ICAM by the end of FY 2018. When the implementation plan was issued in March 2017, the Department had just begun the process of reviewing its needs and requirements for an enterprise-level solution to achieve ICAM requirements that can be used to support the multitenant and multifaceted mission of the Department. Current logical access control system capabilities are not centrally managed or provisioned and there is limited to no information sharing of identity or security entitlement/privilege for the community of users that the applications serve. The Department was still working to understand what would be needed, including resources, to make the ICAM program mature. Further, the Department is assessing the potentially significant resource requirements to monitor users from colleges, universities, and business partners that have access to its systems. Without the full implementation of the ICAM strategy, the Department cannot ensure full accountability of its access management program.

Network Access Control Solution Not Fully Implemented

We found that the Department's network access control solution had not been fully implemented. In January 2014, the Department contracted NTT to implement the network access control solution to (1) identify all devices that are connected to the Department's networks, (2) distinguish server/network/printer/phone devices from end user devices, (3) authenticate devices that connect to the network, and (4) enforce Department-defined endpoint network access control security policies. As outlined previously, our testing confirmed that the Department's network access control was not fully implemented. Also, the Department's 2017 Quarter 3 FISMA report confirmed that the network access control solution had not been fully implemented. Without full implementation of the network access control solution, the Department cannot enforce access security to its information resources.

[16] A privileged user is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. As results of the elevated access, privileged users could control and assign access to others, which create a risk within itself.

[17] On September 8, 2017, the OIG was notified that the final 140 users had their access removed; however, the investigation is ongoing.

The Department's Controls Over Database Management Needs Improvement

We performed database assessments that identified vulnerabilities, configuration errors, and access issues for databases residing in 7 of our 10 judgmentally selected system sample—the NCES Longitudinal Studies; I3Community of Practice and Public Information System Website; Promise Neighborhood Website; OSEP Personnel Development Program Data Collection System; Individuals with Disabilities Education Act Analysis, Communication, Dissemination, and Meetings; Civil Rights Data Collection Reporting Web Site; and Office of General Counsel Case Activity Management System systems. [18]

Our scans of databases associated with these systems identified a total of 30 high vulnerabilities, 74 medium vulnerabilities, and 96 low vulnerabilities. The vulnerabilities were shared with OCIO for remediation. By allowing these vulnerabilities to exist within its database, the Department increases the risk that data can be accessed or altered by unauthorized individuals.

Two-Factor Authentication Had Not Been Fully Implemented

The Department and FSA did not consistently enforce the use of two-factor authentication. We were provided a list of 478 connections for the Department and FSA. Out of the 478 Department and FSA connections, we found 11 connections that were not configured to use two-factor authentication; they connected to Department resources using a single-factor limited to a user name and a password. Of the 11 connections, 6 are used to house student financial and academic data and are considered sensitive. We found similar conditions in our FYs 2011 through 2016 FISMA audits. Although the Department's corrective action plans stated that this finding was addressed in April 2017, we still found connections that did not require two-factor authentication. Enabling two-factor authentication will better ensure that user authentication will be protected to avoid unauthorized individuals accessing Departmental 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, and personnel security policy and procedures; (2) account management; (3) system use notification; (4) remote access; (5) rules of behavior; (6) position risk designation; (7) personnel screening; (8) access agreements; and (9) information system monitoring.[19] The lack of internal controls and safeguards governing the identity and access management could result in increased risk of system compromise.

[18] NCES Longitudinal Studies, I3Communicty of Practice and Public Information System Website, Promise Neighborhood Website, and OSEP Personnel Development Program Data Collection System databases are managed by Westat; the Individuals with Disabilities Education Act Analysis, Communication, Dissemination, and Meetings database is managed by American Institute for Research; and Civil Rights Data Collection Reporting Web Site and Office of General Counsel Case Activity Management System databases are managed by NTT.

[19] Includes control numbers AC-1, AC-2, AC-8, AC-17, IA-1, PL-4, PS-1, PS-2, PS-3, PS-6, and SI-4.

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, in cooperation with the Office of Management, that background investigations are conducted (1) before granting access to Departmental and FSA systems and (2) to ensure the correct level of access is granted.

3.3 Prohibit contractors from granting access to FSA systems without approval by the Department.

3.4 Enforce a two-factor authentication configuration for all user connections to systems and/or applications housing personally identifiable information.

We recommend that the Deputy Secretary require to OCIO—

3.5 Ensure the Department's ICAM strategy is fully implemented to ensure that the Department meets full Federal Government implementation of ICAM.

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

3.7 Create POA&Ms to remedy database vulnerabilities for all database vulnerabilities identified.

We recommend that the Chief Operating Officer require FSA to—

3.8 Establish a process for identifying, managing, and tracking activity of privileged user accounts.

Management Comments

The Department concurred with recommendations 3.1 to 3.5, 3.7 and 3.8, and partially concurred with recommendations 3.6. The Department stated it will develop corrective action plans for these recommendations by December 1, 2017, to address the associated findings.

The Department partially concurred with recommendation 3.6. The Department stated that it had completed the implementation plan of the network access control solution during FY 2017. The Department recognized that during the OIG's testing, the OIG discovered configuration issues. The Department stated that it will develop a corrective action plan by December 1, 2017, to address the associated finding.

OIG Response

The OIG will review the corrective action plans to determine whether the actions will address the findings and recommendations and, if so, will validate them during our FY 2018 FISMA audit.

Regarding recommendation 3.6, the OIG agrees to provide the background information to assist OCIO in validating the finding. Once the corrective action plan is developed, the OIG will review it to determine whether the actions will address the finding and recommendation and, if so, will validate them during our FY 2018 FISMA audit.

METRIC DOMAIN 4—SECURITY TRAINING

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

We determined that the Department's Security Training program was consistent with the Defined level of the maturity model. The Department and FSA defined and appropriately communicated the roles and responsibilities of all of the stakeholders. The stakeholders include all of the Department's employees, OCIO management, FSA management, Federal managers, Department managers, Information Systems Security Officers, Authorizing Officials, and contractors, as well as the authorized officials and CIOs. However, while the Department has made several improvements to its Security Training program, its practices in several areas still do not meet the Managed and Measurable threshold under the metrics to be considered effective. To meet Managed and Measurable, the Department would need to achieve that level in at least 4 of the 6 metric areas. For example, the Department would need to demonstrate that it has addressed all of its identified knowledge, skills, and abilities gaps. It would also have to demonstrate that skilled personnel have been hired and/or existing staff trained to develop and implement the appropriate metrics to measure the effectiveness of the organization's training program in closing identified skill gaps.

The Department established the "Information Technology Cyber Security Awareness and Training Program Guidance," dated February 2016. This program informs personnel, including contractors and other users of information systems that support the operations and assets of the agency, of information security risks associated with their activities and their responsibilities in complying with Department policies and procedures designed to reduce these risks. One of the primary goals of the program is to reduce risk to Department systems and information assets by changing human behavior.

The Department established a Cybersecurity Workforce Development working group that is headed by the Chief Information Security Officer. The purpose of that group is to develop a strategy plan to help ensure that cybersecurity workforce development is successful at the enterprise level. In May 2017, the OCIO, Information Assurance Services, established the Cybersecurity Workforce Development Strategy and Program Plan. The plan is intended to be

fully aligned with the Federal Cybersecurity Workforce Strategy that was issued by OMB on July 12, 2016, via OMB Memorandum M-16-15. The plan details the Department's actions to identify, expand, recruit, develop, retain, and sustain a capable and competent workforce in key functional areas to address complex and ever-evolving cyber threats.

The OCIO, Information Assurance Services, established an "Information Technology Cyber Security Awareness Program Tactical Plan for Fiscal Years 2017-2018," dated July 2017. The mission of the IT Security Awareness and Training Program is to provide current and relevant cybersecurity awareness, education and training to employees, contractors and other users of information systems that support the operations and assets of the Department. The program focuses on changing human behaviors by informing personnel of their responsibilities in complying with Department policies and procedures, is designed to reduce risks, and supports the continuous growth and development of the cybersecurity workforce.

In July 2017, the OCIO established its "Cybersecurity Certification Program Guidance for ED Information Technology Professionals." The program details Department-wide actions to comply with the requirements of the Federal Cybersecurity Workforce Assessment Act. This Act requires Federal agencies to conduct and report on a baseline assessment of the existing cyber workforce by identifying (1) the percentage of staff with cyber functions who currently hold appropriate certifications, (2) the level of preparedness of staff without credentials to take certification exams, and (3) a strategy for mitigating any gaps identified.

We found that the Department established a process for suspending user accounts that have not completed the required security training by a defined date. This process was established for both Federal and contractor employees.

The Department conducts simulated phishing exercises that measure the number of users who open or read the phishing email and download and view the attachment. We reviewed the Department's tracking data of the exercises conducted from October 2014 through May 2017 and identified a decreasing trend in both Departmental employees and contractors who downloaded and viewed the attachment.

Issue 4. The Department's Security Training Program Needs Improvement

Of the six metrics for the Security Training domain, we found the Department and FSA to be at the Defined level for all six metrics.

We found that contractors were able to obtain access to Departmental resources before fulfilling their training requirements. For the first quarter of FY 2017, we found that out of 212 contractor accounts, 88 (42 percent) had access to Departmental resources before completing required training. Further, for the second quarter of FY 2017, we found that out of 341 contractor accounts, 186 (55 percent) had access to Departmental resources before completing training. Currently, the Department does not have a process to verify that contractors completed the required security training and rely on the system owners to provide evidence that this has occurred. In addition, the Department relies on system owners to enforce security training to its contractors relating to suspending, terminating, and removing access to its network.

OMB Circular A-130, Appendix III, "Management of Federal Information Resources," requires that all individuals be appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. Further, the Department's "Information Technology Cyber Security Awareness Training Guidance," requires assurance that all users of its systems (i.e., general support systems and major applications) are appropriately trained in how to fulfill their security responsibilities before allowing them access to systems. NIST SP 800-50, "Building an Information Technology Security Awareness and Training Program," Section 1.5.2, requires CIOs to ensure that effective tracking and reporting mechanisms for security training are in place. Without a formal process for educating contractors about IT security, the Department has no assurance that its workforce will fulfill their security responsibilities.

Recommendations

We recommend that the Deputy Secretary require OCIO to—

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

4.2 Ensure that contractors fulfill mandatory training requirements before accessing Departmental systems.

Management Comments

The Department concurred with the recommendations. The Department stated it will develop a corrective action plan by December 1, 2017, to address the associated finding.

OIG Response

The OIG will review the corrective action plan to determine whether the actions will address the finding and recommendations and, if so, will validate them during our FY 2018 FISMA audit.

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 categorized as being not effective. We found that the Department and FSA established policies and procedures with NIST guidelines and OMB policy, finalized the implementation of Phase 1 of the DHS CDM program, established the Cybersecurity Risk Management Framework, use the results of security control assessments and monitoring to maintain ongoing authorizations of information systems, and conducted Quarterly Cybersecurity Risk Management Forums and Workshops. However. we noted some improvements are needed to help the agency reach a higher level of maturity. For instance, we found improvements are needed in security control monitoring, developing and identifying roles and responsibilities, and fully implementing the CDM program.

METRIC DOMAIN 5—INFORMATION SECURITY CONTINUOUS MONITORING

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

In FYs 2015 and 2016, we determined that the Department's and FSA's ISCM program was at Level 1: Ad Hoc of the maturity model. Specifically, for 2016, we found that the Department and FSA did not meet Level 2 requirements because the Department and FSA (1) did not assess the skills, knowledge, and resources needed to effectively implement an ISCM program (at both Level 1 and Level 2) and (2) did not define ISCM stakeholders and their responsibilities and communicated this across the organization.

This year we determined that the Department's and FSA's ISCM programs were consistent with the Defined level of the maturity model. The Department and FSA perform ongoing assessments of their systems to grant authority to operate. They use the Cyber Security Assessment and Management system to store, monitor, and track the status of the system security authorization documentation for each of the Department's systems. However, while the Department has made several improvements to its ISCM program, its practices in several areas still do not meet the Managed and Measurable threshold under the metrics to be considered effective. The Department and FSA have all the capabilities and resources to transition to the next maturity level; however, to meet Managed and Measurable level, the Department would need to achieve that level in at least 2 more of the 5 metric areas. For example, the Department would need to demonstrate that its staff is 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.

The Department has taken steps to strengthen its ISCM program. For instance, the Department initiated and completed a self-assessment of its ISCM program and rated themselves at the Defined maturity level. The Department also finalized and implemented Phase 1 of the DHS CDM program. This process is aligned with the Department's ISCM program and was implemented in July 2017. In addition, as part of Phase 1 of the CDM program, the Department updated its vulnerability and patch management procedures, configuration management guidance, and hardware and software management guides.

In January 2016, the Department created the Cybersecurity Risk Management Framework to allow the stakeholders to manage risk. The Cybersecurity Risk Management Framework is used to evaluate the organization risk posture, the maturity of the agency cyber security program, vulnerabilities, security program life cycle, and governance of the security program. The Department has incorporated some portions of the Framework into its ISCM program. Also, the Department's EARB is integrated with the Cybersecurity Risk Management Framework and Enterprise Architecture Process.

The Department and FSA use the results of security control assessments and monitoring to maintain ongoing authorizations of information systems. FSA has the Ongoing Security Authorization program and the OCIO has the Continuous Security Authorization program. Both programs were designed to authorize systems and continually monitor them through their life

cycle as opposed to the former certification and accreditation process. FSA has been operating its Ongoing Security Authorization program since FY 2013, and OCIO has been operating its Continuous Security Authorization program since FY 2014. The Department and FSA use the CSAM system to monitor and manage the authorization process for their systems. CSAM also acts as a repository for all security documentation and POA&Ms, along with risk acceptance justifications.

The Department uses performance metrics and lessons learned in collaboration with its stakeholders as a way to determine whether the ISCM program is fully integrated. The Department also conducts Quarterly Cybersecurity Risk Management Workshops that provide resources and references that enable stakeholders to address CSAM Risk Management Framework checklists. These workshops cover issues such as (1) common control identification, (2) security control selection, and (3) security plan approval. The Department also conducts Quarterly Cybersecurity Risk Management Forums for stakeholders to discuss program governance, risk, and compliance. These forums cover issues such as (1) IT system assessments, (2) ISCM, (3) cybersecurity policy and guidance updates, (4) authorization to operate statuses, (5) POA&Ms by principal office, (6) transport layer security, (7) unauthorized software, (8) fiscal year assessment schedule, and (9) CSAM monitoring. In addition, the Department is meeting weekly to discuss major milestones and enforcement. The Department also uses these forums to discuss ongoing challenges, such as encryption requirements for publically accessible websites, and system stakeholders' understanding of POA&M root causes and how to identify proper actions to remediate these challenges.

Issue 5. The Department's ISCM Program Needs Improvement (Repeat Finding)

Of the five metrics for the ISCM program domain, we found the Department and FSA to be at the Defined level for three metrics, the Managed and Measurable level for one metric, and the Consistently Implemented level for one metric. We found that the Department can strengthen its controls regarding ISCM, which will enable it to progress to the next maturity level in the areas of (1) security control monitoring, (2) developing and identifying roles and responsibilities, and (3) fully implementing its CDM program.

Department Relies on Manual Security Control Monitoring

The Department's latest revision of its ISCM Roadmap (April 2017) encompasses people, policies, processes, and technology and is used to perform ISCM as defined by NIST. It supports ongoing observation, assessment, analysis, and diagnosis of an organization's information security posture, hygiene, and operational readiness. Although the Department has improved capabilities on monitoring the security controls effectiveness and improving overall implementation on a continuous basis, it currently relies on manual processes. It is the Department's goal to become more automated with the assistance of CSAM.

ISCM Stakeholders With Designated Roles and Responsibilities Need Further Engagement

Although the Department's ISCM Roadmap details the roles and responsibilities that will enable the ISCM program to be successful, it is still in the process of trying to better educate and engage ISCM stakeholders. For instance, the Department has assessed skills for specific roles at the enterprise level such as the Authorizing Official, Chief Information Security Officer, Information

System Security Officer, and System Owners; however, knowledge of their ISCM roles and responsibilities were limited. Also, new roles have been created that currently require a staff member to assume dual roles. In addition, the Department identified 126 operational systems across the agency with required Information System Security Officers that do not have a CSAM account or are missing a required point of contact.

CDM Program Not Fully Implemented

As a participant in the DHS CDM program, the Department can leverage DHS' technical architecture for the CDM system.[20] As of June 2017, the Department had completed Phase 1 of the three-phase program where it has aligned DHS policies and procedures with its ISCM program. With Phase 1 of the program implemented, the Department was participating in Phase 2 of the CDM program. However, at the time of our fieldwork, the Department was only in the planning stage and had not completed implementation.

In accordance with NIST SP 800-137, communication with all stakeholders is key in developing the ISCM strategy and implementing the program. This standard builds on the monitoring concepts introduced in NIST SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems." An ISCM program helps ensure that deployed security controls continue to be effective and operations remain within organizational risk tolerances despite inevitable changes that occur over time. In cases where security controls are determined to be inadequate, ISCM programs facilitate prioritized security response actions based on risk.

By implementing an automated security control process, establishing roles and responsibilities in its ISCM program, and successfully implementing the CDM program, the Department can help ensure that it maintains an effective ISCM program for its deployed security controls.

Recommendations

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

5.1 Incorporate additional measures to, at a minimum, achieve Level 4 Managed and Measurable status of the ISCM program.

We recommend that the Deputy Secretary require OCIO to—

5.2 Automate its capabilities for monitoring the security controls effectiveness and overall implementation of the ISCM Roadmap.

5.3 Ensure that ISCM stakeholders with designated roles and responsibilities are properly educated and engaged.

[20] A CDM system provides continuous diagnostics and mitigation and provides the results and analysis of these diagnostics to dashboards at the agency level and at the Federal level.

5.4 Ensure all Information System Security Officers establish and use CSAM accounts, and that required points of contacts are identified.

5.5 Ensure the completion of Phase 2 of the CDM program.

Management Comments

The Department concurred with the recommendations. The Department stated it will develop a corrective action plan by December 1, 2017, to address the associated finding.

OIG Response

The OIG will review the corrective action plan to determine whether the actions will address the finding and recommendations and, if so, will validate them during our FY 2018 FISMA audit.

SECURITY FUNCTION 4—RESPOND

The "Respond" security function comprises the Incident Response metric domain. Based on our evaluation of the Department's Incident Response program, we determined the Respond security function was at Defined level of the maturity model, which is categorized as being not effective. We found that the Department established policies and procedures consistent with NIST guidelines and OMB policy, established an incident response process, developed a Security Operations Center process, performed tabletop exercises, participated in the DHS EINSTEIN program, deployed numerous incident response tools, and produced monthly status reports. However, we noted some improvements are needed to help the agency reach a higher level of maturity. For instance, we found (1) Departmental guidance needed to be updated, (2) training is needed for key personnel, (3) incidents were not reported in a timely manner, and (4) the EINSTEIN interconnection security agreement was not current.

METRIC DOMAIN 6—INCIDENT RESPONSE

An organization's incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited to prevent future occurrences, and restoring IT services. The goal of the incident response program is to (1) provide surveillance, situational monitoring, and cyber defense services; (2) rapidly detect and identify malicious activity and promptly subvert that activity; and (3) collect data and maintain metrics that demonstrate the impact of the Department's cyber defense approach, its cyber state, and cyber security posture.

We determined that the Department's Incident Response programs were consistent with the Defined level of the maturity model. The Department had the policies and procedures to determine the knowledge, skills, and abilities of its workforce; had a situational awareness of vector taxonomy; and developed lessons learned which provided them with the understanding of how their effectiveness of the incident handing process could be improved. However, while the Department has made several improvements to its Incident Response program, its practices in several areas still do not meet the Managed and Measurable threshold under the metrics to be considered effective. To meet Managed and Measurable, the Department would need to achieve

that level in at least 4 of the 7 metric areas. For example, the Department would need to demonstrate that it has the ability to manage and measure the impact of successful incidents and is able to quickly mitigate related vulnerabilities on other systems so that they are not subject to exploitation of the same vulnerability.

In FY 2016, CIGIE, in coordination with OMB and DHS, developed the Incident Response maturity model. Our evaluation of the FY 2016 Department's Incident Response program determined that the Respond security function was at Level 1: Ad-hoc, which was categorized as being not effective. Specifically, the Department and FSA did not have documented policies and procedures, inconsistently implemented incident handling procedures for security events, and had not implemented incident response technologies.

The Department established OCIO Handbook-14, "Information Security Incident Response and Reporting Procedures" to provide incident response and reporting procedures to ensure appropriate and expeditious handling of information security incidents that may affect the Department's normal business operations. These procedures define the Department's incident response and reporting process as well as roles and responsibilities.

The Department has defined and communicated the structures of its incident response teams and their roles and responsibilities. It created the "Education Security Operations Center Roles and Responsibilities Standard Operating Procedures," which distinguished tier responsibilities for the Education Security Operations Center (EDSOC) analyst. The EDSOC engineer provides maintenance and updates of the architecture of the SOC infrastructure that includes controlling and managing the life cycle of all SOC changes, and ensures that hardware and software are operational. The Change and Release Management component oversees and manages the production and testing environments that includes the shared application and technical services and well as the data centers.

The Education Computer Incident Response Capability Coordinator confirmed that addressing each threat event differs depending on the type of incident and that there is a process to address the incident at each level. For instance, a security event would be evaluated to determine the reporting parameters, identify the source, identify the threat vector, and determine how to quarantine the incident. The Education Computer Incident Response Capability Coordinator is notified of the incident by the SOC coordinator, and the incident documentation is forwarded to the CIO, the Chief Information Security Officer, system owner, and sometimes the Information System Security Officer. The EDSOC team is responsible for performing the containment and eradication activities. The team works with the stakeholders to establish corrective actions and develop mitigation strategies, including any further escalation procedures with the OIG's Technology Crimes Division. For external systems, the Department uses a team collaboration method that involves Department personnel, third parties, and system liaisons to work with system owners to remediate security incidents.

Although the EDSOC facility is not considered a Sensitive Compartmented Information Facility, it has established this functionality that is currently certified and accredited for Top Secret/Sensitive Compartmented Information processing. The EDSOC Sensitive Compartmented Information Facility was certified in January 2015.

To address the effectiveness of the incident response program, both the Department's and FSA's SOCs participated in tabletop exercises that provided stakeholders an opportunity to walk through the incident response process and procedures using actual incident scenarios and testing of breach responsiveness. In June 2016, the Department conducted a tabletop incident response exercise on how it would respond to a breach of personally identifiable information. Lessons learned from the exercise were documented and table top exercises are now performed annually.

The Department participates in DHS' EINSTEIN Program. The EINSTEIN system is a collection of tools that is used across the Federal Government to provide an automated process for the U.S. Computer Emergency Readiness Team (US-CERT) to collect, analyze, and share cyber threat information throughout the Government. This program provides the Department with real-time alerts on potential cyber threats on its network and increases its situational awareness for incident response.

The Department has acquired and implemented incident response tools to extract data and to identify cyber threat indicators. These tools provide the Department with the support needed for monitoring and analyzing qualitative and quantitative data. Alerts are actively monitored from the different tools and the Department validates the cyber threat indicators from US-CERT and identifies any false positives. For both the Department's and FSA's SOCs, daily meetings are conducted to discuss incident activities.

The Department established monthly program status reports that enabled it to share incident activities with internal stakeholders. The report contains quantitative and qualitative data that provides the Department with a snapshot status of what was accomplished. For instance, the EDSOC Coordinator can see how well Service Level Agreements are being achieved regarding security engineering, vulnerability management, and EDSOC incident handling. We obtained monthly program status reports for January through June 2017 that showed status of reported incidents and data loss prevention events.

Issue 6. The Department's Incident Response Program Needs Improvement (Repeat Finding)

Of the seven metrics for the Incident Response domain, we found the Department to be at the Defined level for five metrics and the Ad Hoc level for two metrics. We found that the Department can strengthen its controls regarding incident response to enable it to progress to the next maturity level in the areas of (1) updating current guidance, (2) training key personnel, (3) the timely reporting of incidents, and (4) maintaining current interconnection security agreements.

Departmental Guidance Was Not Updated

We found that OCIO Handbook-14, "Information Security Incident Response and Reporting Procedures," dated March 2011, was being updated and was under review by OCIO. We were informed that the draft Handbook was in compliance with NIST guidance and will serve as the Department's enterprise level Cybersecurity Incident Response Plan. The Handbook will consist of the Incident Management Lifecycle, which provides the process to identify, analyze, and contain incidents, and the Incident Management Framework, which implements the life cycle and is a collection of practices and tools that prioritize, categorize, track, assign, document, and

communicate to ensure that incident response activities are organized and maintained. At the time of our review, the draft was in the Administrative Communication Systems process for approval.

Incident Response Training for Key Personnel

Although the Department identifies specific training for general system users on how to prevent security incidents, it does not establish specific training for key personnel whose role and responsibility it is to respond to incidents when they occur. The Department views the EDSOC team as incident responders, rather than general system users. OCIO-14, "Information Security Incident Response and Reporting Procedures," does not identify incident response training for key personnel. However, the Department is developing a formal training process that is captured in its Cyber Workforce Development Program that will identify the knowledge, skills, and abilities needed for incident response. In addition, the Department is looking to incorporate incident response training requirements that would require key stakeholders to obtain specific security certifications.

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

According to US-CERT Federal Incident Notification Guidelines, EDSOC 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, SOC, or IT department. This reporting timeline was adopted and incorporated into the Department's overarching incident response policies and procedures—"Handbook for Cybersecurity Incident Response and Reporting Cyber Security Operations Standard Operating Procedures." The Handbook requires the Department to report all incidents identified as Categories 1 through 4 to the OIG.[21] Our testing found that the Department was not submitting incidents to US-CERT within the required timeframes, nor communicating them to the OIG. To conduct our testing, we obtained the Department's computer security incident report log, which identified 1,062 incidents that occurred from October 2016 through April 2017. Of the 1,062 incidents, 127 were identified as required to be submitted to US-CERT.[22] However, we found that 26 of the 127 incidents were not submitted within the required reporting guidelines. One category 1 incident was reported 27 days after it occurred. Furthermore, out of 188 incidents (41 category 1 incidents and 147 from categories 2 through 4), only 3 incidents were actually reported to the OIG, as required.

Interconnection Security Agreement Not Current

The Department's Interconnection Security Agreement (ISA) for participation in the DHS' EINSTEIN program is not current. US-CERT provided the ISA agreement to OCIO for the deployment of EINSTEIN collectors and intrusion detection devices for all internet gateways owned by the Department to help identify and mitigate malicious activity. The ISA between DHS and the Department was initiated in June 2009 and stated that the document would be

[21] Category 1 is defined as unauthorized access. Category 2 is defined as a denial of service. Category 3 is defined as malicious code. Category 4 is identified as improper usage.
[22] The remainder of the 900 incidents we reviewed complied with the reporting timelines.

reissued every 3 years. In 2017, we found that despite this requirement, the Department continues to rely on its 2009 version. The Department is required to follow up with US-CERT to renew the ISA and has not done so.

OMB and NIST guidelines[23] speak to several requirements for implementing an effective incident response program. Adhering to the guidelines allows for the 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 IT systems.

Recommendations

We recommend that the Deputy Secretary require OCIO to—

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

6.2 [Removed after Department's response]

6.3 Establish a specific training curriculum for key personnel who respond to incidents when they occur.

6.4 Ensure that incidents are submitted to US-CERT within the required timeframe and all incidents identified as Categories 1 through 4 to the OIG that could possibly relate to cyber fraud.

6.5 [Removed after Department's response]

Management Comments

The Department concurred with recommendations 6.1, 6.3, and 6.4. The Department stated it will develop a corrective action plan by December 1, 2017, to address the associated finding.

The Department partially concurred with recommendations 6.2 and 6.5. For recommendation 6.2, the Department stated that although it was not published during the course of the audit fieldwork, the updated handbook was signed on September 27, 2017. For recommendation 6.5, the Department stated that although it was not published during the course of the audit fieldwork, the ISA for the EINSTEIN program was updated on October 12, 2017. OCIO provided a copy of this document to OIG.

[23] 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.

OIG Response

The OIG will review the corrective action plans to determine whether the actions will address the finding and recommendations and, if so, will validate them during our FY 2018 FISMA audit.

Regarding recommendation 6.2, the OIG obtained a copy of the document and confirmed that it was published on that date. The OIG concluded that OCIO's actions satisfy the recommendation and no further corrective actions are needed.

Regarding recommendation 6.5, the OIG concluded that OCIO's actions satisfy the recommendation and no further corrective actions are needed.

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 Defined level of the maturity model, which is categorized as being not effective. We found that the Department and FSA established policies and procedures consistent with NIST guidelines and OMB policy; maintained recovery strategies, plans, and procedures at the organization and application level; developed a comprehensive disaster recovery process; and maintained a centralized repository for storing and tracking contingency planning documentation. However, we noted some improvements are needed to help the agency reach a higher level of maturity. For instance, we found improvements are needed in enterprise skill assessment and contingency plan documentation.

METRIC DOMAIN 7—CONTINGENCY PLANNING

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

In FY 2016, the Contingency Planning maturity model was not developed for this metric. Therefore, the Department and FSA were measured against less restrictive maturity model indicators, and the Department's contingency planning program was scored at Level 5: Optimized, considered effective. Specifically, the Department and FSA established policies and procedures consistent with OMB policy and applicable NIST guidelines; maintained recovery strategies, plans, and procedures at the organization and application level; developed a comprehensive disaster recovery process; and considered supply chain threats as part of their contingency planning process.

The FY 2017 FISMA Metrics include a more restrictive maturity model for the Contingency Planning, based on which we determined that the Department has established and maintains an enterprise-wide business continuity/disaster recovery program. Furthermore, we identified that contingency planning and contingency plan testing are performed at the application level.

We determined that the Department's and FSA's Contingency Planning programs were consistent with the Defined level of the maturity model. For example, the roles and responsibilities of stakeholders involved in information system contingency planning have been fully defined and communicated across the organization. The Department has also defined appropriate teams that are ready to implement its information system contingency planning strategies. However, while the Department has made several improvements to its Contingency Planning program, its practices in several areas still do not meet the Managed and Measurable threshold under the metrics to be considered effective. To meet Managed and Measurable level, the Department would need to achieve that level in at least 4 of the 7 metric areas. For example, the Department would need to demonstrate that it employed automated mechanisms to more thoroughly and effectively test system contingency plans.

The Department has defined policies, procedures, and strategies, as appropriate, for information system contingency planning, including technical contingency planning considerations for specific types of systems, such as cloud-based systems, client/server, telecommunications, and mainframe-based systems. Areas covered include, at a minimum, roles and responsibilities, scope, resource requirements, training, exercise and testing schedules, plan maintenance schedules, backups and storage, and use of alternate processing and storage sites. "Information Technology Contingency Planning Guidance, Version 1.1," dated February 2016, provided Department-level guidance for the development and maintenance of contingency plans to include the notification/activation procedures, as well as capturing test results and lessons learned for incorporation into the contingency plan and future test plans. This guidance was also consistent with NIST 800-34, "Contingency Planning Guide for Federal Information Systems." Both internal and external contractors involved in the contingency planning process are required to comply with Departmental policies and guidance and must ensure that their internal processes meet the Department's policy requirements. Enforcement is validated through the security authorization process, annual testing, evaluations, and third-party assessments.

The Department publishes guidance for developing and maintaining contingency plans and for conducting contingency plan tests to promote consistency in the applicable contingency plan elements. We found that the Department established contingency plan and contingency plan testing templates for the development and maintenance of contingency plans, and contain all the required NIST elements that are provided to all shareholders. The Department's contingency planning guidance requires that contingency plans be updated at least annually or whenever significant changes to a system occur.

The roles and responsibilities for contingency planning and testing are defined and communicated across the organization, as well as to all of the relevant stakeholders, and are captured in the Department's "Information Technology Contingency Planning Guidance, Version 1.1," dated February 2016, consistent with NIST 800-34, "Contingency Planning Guide for Federal Information Systems." For instance, each principal office is responsible for the development of a Business Continuity Plan and Disaster Recovery Plan, and the Continuity Manager is responsible for developing and maintaining a Continuity of Operations Plan.

The Department stated that it had established role-based training at the enterprise level for those individuals with specific responsibilities for contingency planning process. The Department is also in the process of evaluating individuals with cybersecurity responsibilities and pairing them

with the relevant type of training according to job function and credentials (in accordance with its Cybersecurity Workforce Development strategy).

We determined that the Department established an annual process to plan, execute, and document disaster recovery results.[24] For FY 2017, we attended planning meetings, as well as monitored the execution of the all-inclusive disaster recovery test of all components of the EDUCATE infrastructure that included two systems from our judgmentally selected system sample. All components were tested simultaneously and all systems were successfully tested, and in accordance with the documented plans and timelines. We confirmed that during the exercise, problems were recorded and tracked and the resolution was formalized, accurate, and appropriately communicated to management. This included documenting lessons learned, as well as a gap analysis. The Department encountered and resolved two issues during the exercise. We also verified that communications with external shareholders occurred through forums and workshops, as well as during the actual exercise, to discuss changes, possible issues, lessons learned, and the overall effectiveness of the recovery activities. Any changes that occur during the testing processes were addressed by the individual system owners and their respective contingency plans were updated to reflect the changes.

We determined that Departmental guidance defines the business impact assessment (BIA) process for correlating specific information resources with the essential services that they provide in its "Information Technology Contingency Planning Guidance, Version 1.1." This enables the Department to determine the consequences of a disruption to the system and the business components by requiring it to identify essential IT resources, identify disruption impacts and allowable outage times, and develop recovery priorities. The BIA is an appendix within the Department's contingency plan template. We verified that the BIA template provided to the externally hosted system owners is consistent with elements cited in Departmental guidance.

Each system and/or application's security documentation is housed within the CSAM tool that includes all contingency planning testing and results. Before annual testing, the Department reviews the lessons learned from the previous test to ensure changes are incorporated within the current test.

Issue 7. The Department's and FSA's Contingency Planning Program Needs Improvement

We determined that the Department's and FSA's Contingency Planning programs were consistent with the Defined level of the maturity model. Of the seven metrics for this domain, we found the Department and FSA to be at the Defined level for five metrics, the Managed and Measurable level for one metric, and the Consistently Implemented level for one metric. We found that the Department can strengthen its controls regarding contingency planning to enable it to progress to the next maturity level in the areas of (1) enterprise skill assessment; (2) documenting contingency plans, BIAs, and contingency plan testing; and (3) contingency plan completeness.

[24] FSA performs disaster recovery exercises biannually.

Enterprise Skill Assessment Not Performed

Although the roles and responsibilities of stakeholders involved in information system contingency planning have been fully defined and communicated across the organization, Department officials acknowledged that the current skill assessment processes occurs at the system-level (individual systems); it is not being measured at the enterprise level. We found that the Department was in the process of establishing a cybersecurity workforce group and aligning the training with certification requirements. At the contractor level, we were also informed that the Department is reviewing all new contracts for specific IT language that addresses hiring of skilled personnel that can support contingency planning activities.

Contingency Plans, BIAs, and Testing Not Consistently Updated or Tested Annually

We found that the Department was not consistent and timely in documenting its system contingency plans, BIAs, and results of contingency plan testing. From our judgmentally selected system sample of 10 systems, we obtained and reviewed each system's contingency plan, BIA, and contingency plan testing results. We determined that 4 of the 10 systems did not have current contingency plans, 2 of the 10 plans did not show that a BIA was conducted, and 7 of the 10 systems did not contain evidence that the plans were annually tested as required by NIST.

Contingency Plans Did Not Contain All Required Information

We found that the Department was not consistently including all required contingency planning information. During our review of the 10 contingency plans, we found that one did not specify identified resources, one did not specify the alternate storage, three did not identify an alternate processing site, three did not identify specific details on testing and training, two contained no specific details on maintenance activities, and four did not have evidence of telecommunication agreements.

During FY 2017, the Department and FSA switched to CSAM as the main and central repository of all systems and applicable documentation. As a result of this transition, all current information may not have been fully uploaded, which could account for missing or outdated information. For our independent testing, we also reviewed system status and system assessment reports within CSAM and determined that the same conditions existed relating to missing or outdated contingency plans and testing documents. In addition, these reports identified that the Department was not complying with applicable security controls (24 percent of the systems 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 establishing contingency plans and contingency plan testing.[25] Without ensuring that skill assessments are performed at the enterprise level, necessary planning and testing documentation

[25] Includes control numbers CP-2 and CP-4.

is maintained, and that plans contain all the required elements, the Department cannot be assured that it will be able to successfully recover all of its IT resources in the event of a disaster.

Recommendations

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

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

We recommend that the Deputy Secretary require OCIO to—

7.2 Ensure that skill assessments are being measured at the enterprise level.

7.3 Ensure that contingency plans, BIAs, and results of contingency plan testing are documented in a consistent and timely manner.

7.4 Ensure that contingency plans include all required information.

Management Comments

The Department concurred with the recommendations. The Department stated it will develop a corrective action plan by December 1, 2017, to address the associated finding.

OIG Response

The OIG will review the corrective action plan to determine whether the actions will address the finding and recommendations and, if so, will validate them during our FY 2018 FISMA audit.

OTHER MATTERS

During 2016 and 2017, we were informed that the Department's and FSA's service contracts for the EDUCATE and the Virtual Data Center computing environments were going to expire and be recompeted. During the audit, we obtained a status on recompete process for both of the contracts.

EDUCATE Recompete Process Status

The EDUCATE contract was awarded in September 2007 and required the delivery of fully managed services that included infrastructure, computers, telecommunications devices, an e-mail network, Department's internet and intranet sites, servers, telephone systems and network printers, and other services and equipment as needed. In May 2016, a six-vendor strategy, called the Portfolio of Integrated Value-Oriented Technologies, was finalized to provide all IT services. Vendors of these services are required to manage migration of their services to replace EDUCATE. Vendor transitions were planned to start in July 2017. The EDUCATE contract expires in November 2017.

Virtual Data Center Recompete Process Status

The Virtual Data Center contract was awarded in 2006 to Dell Services Federal Government to provide data center services and expired in August 2016. In 2013, a high-level strategy was developed to revisit service-level agreements to improve system availability, quality of service, performance, tracking, and reporting. The contract was recompeted in 2015 as the Project Phoenix/Next Generation Data Center and awarded to Hewlett-Packard Enterprise Services. The Security Authorization Decision to operate was signed by the CIO and the Deputy CIO on July 11, 2017. During the transition from the Virtual Data Center to the Next Generation Data Center, we determined that physical and environmental controls, as well as continuity measures, are in place and effective to support the Department's security program and practices.[26] We performed a physical and environmental control assessment of the new data center facility.

Although contracts were awarded to new vendors, it is imperative that the Department and FSA ensure that the audit findings associated with the systems we tested for this audit, as well as previous audits, are adequately addressed so that these same deficiencies do not continue in the new computing environments. Specifically, since systems will be in new environment and will require new security documentation, any past deficiencies need to be systemically addressed so that future OIG IT security audits do not encounter and report the same deficiencies as repeat findings.

[26] To the extent possible, we assessed physical and environmental controls, as well as continuity measures, in place against NIST SP 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations, Physical and Environmental Protection Control Family."

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine whether the Department's and FSA's overall IT security programs and practices were effective as they relate to Federal information security requirements. For FY 2017, the IG reporting metrics were organized around the five information security functions outlined in the NIST's Framework for Improving Critical Infrastructure Cybersecurity: Identify, Protect, Detect, Respond, and Recover. To meet the objective, we conducted audit work and additional testing in the seven metric domains associated with the security functions identified in the framework: (1) Risk Management (2) Configuration Management, (3) Identity and Access Management, (4) Security Training, (5) Information Security Continuous Monitoring, (6) Incident Response, and (7) Contingency Planning.

To accomplish our objective, we performed the following procedures:

- reviewed applicable information security regulations, standards, and guidance;
- gained an understanding of IT security controls by reviewing policies, procedures, and practices that the Department has implemented at the enterprise and system levels;
- assessed the Department's enterprise- and system-level security controls;
- interviewed Department officials and contractor personnel, specifically staff with IT security roles, to gain an understanding of the system security and application of management, operational, and technical controls;
- gathered and reviewed the necessary information to address the specific reporting metrics outlined in DHS's FY 2017 IG FISMA reporting 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:

- system-level testing for the Configuration Management, Risk Management, and Contingency Planning metrics;
- review of OCIO's Security Control Assessment and FSA's Ongoing Security Authorization programs;
- vulnerability assessment testing of HEAL Online Processing System; IES Data Center; Individuals with Disabilities Education Act Analysis, Communication, Dissemination, and Meetings; NCES Longitudinal Studies; I3Community of Practice and Public Information System Website; Civil Rights Data Collection Reporting Web Site; Office of General Counsel Case Activity Management System; Promise Neighborhood Website; and OSEP Personnel Development Program Data Collection System systems, applications, and infrastructure;
- verifying training evidence and completion;
- verifying security settings for the Department data protection; and
- observing the all-inclusive EDUCATE disaster recovery exercise.

As of February 2017, the Department identified an inventory of 134 systems that are FISMA reportable and classified as operational. Out of the 134 FISMA reportable systems, 2 systems were classified as high-, 94 as moderate-, and 38 as low-impact systems. Because of the Department's and FSA's current transition of EDCUATE and Virtual Data Center's systems to

new hosting environments, we primarily focused on externally hosted systems. We judgmentally selected 8 of the 83 externally hosted FISMA reportable systems. In addition, we judgmentally selected two internal systems that were never selected for review in previous years' FISMA audits. In making our selection, we considered risk-based characteristics such as system classifications (high, moderate, and low), those systems containing personally identifiable information, and geographical location of the hosted systems.

The table below lists the judgmentally selected systems, the system's principal office, and the Federal Information Processing Standards Publication 199 potential impact level.[27]

Number	System Name	Principal Office	Impact Level
1	HEAL Online Processing System	FSA	Moderate
2	IES Data Center	IES	Moderate
3	Individuals with Disabilities Education Act Analysis, Communication, Dissemination, and Meetings	OSERS	Low
4	NCES Longitudinal Studies	IES	Moderate
5	I3Communicty of Practice and Public Information System Website	OII	Moderate
6	Civil Rights Data Collection Reporting Web Site	OCR	Moderate
7	Office of General Counsel Case Activity Management System	OGC	Moderate
8	Promise Neighborhood Website	OII	Moderate
9	TRIO Programs Annual Performance Reports Data Collection and Processing Applications	OPE	Moderate
10	OSEP Personnel Development Program Data Collection System	OSERS	Low

These systems helped us ascertain the security control aspects relating to Configuration Management, Risk Management, and Contingency Planning.[28] In addition, these systems were the focus of our system vulnerability assessment and testing.

In addition to the sample of 10 systems, we also used sampling to test certain aspects in the areas of risk management, configuration management, incident response, and security training. For risk management, we tested all of the 987 POA&Ms for the timeframe of October 2016 through April 2017. For configuration management, we tested all 478 Departmental websites for secure configurations for hypertext transfer protocol connection; login credentials; inventory counts; protection of personally identifiable information; and obsolete systems, applications, and databases; we focused on 11 connections with no mechanism for two-factor authentication. For

[27] 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.

[28] Because we did not select a statistical random sample, any results found during our analysis were not projected across the entire inventory of Department IT systems.

252 out of the 478 Departmental websites associated with the EDUCATE environment, we tested for secure socket layer connection and login banner compliance. For incident response, we tested all 1,062 incidents that occurred from October 2016 through April 2017. For security training, we tested all 212 new user accounts created from November 2016 through December 2016, as well as all 341 new user accounts created from October 2016 through March 2017. We also requested additional details and tested a representative sample of 3 users from each month, for a total of 12 out of the 66 new user accounts created from January 2017 through April 2017. In addition, we reviewed all 19 Department employee accounts, as well as 648 contractor accounts subject to suspension for noncompliance with training requirements during the months of December 2016 and February 2017, and as of March 2017, respectively. Where we relied on judgmental sampling and auditor judgment, we did not project the results from the above samples.

For this audit, we reviewed the security controls and configuration settings for systems and applications and at the NTT facility,[29] the Health and Human Services Facility,[30] Amazon Web Services,[31] American Institute for Research,[32] and Westat.[33] We used computer-processed data for the Risk Management, Configuration Management, Identity and Access Management, and Security Training metrics to support the findings summarized in this report. We also performed an assessment of the computer-processed data and determined these 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 was verified to source and tested for accuracy according to relevant system controls until enough information was available to make a reliability determination. We also performed an assessment of the computer-processed data and determined this data was reliable for the purpose of our audit. We conducted our fieldwork from February 2017 through August 2017, primarily at Department offices in Washington, D.C., and contractor facilities in Plano, Texas; Rockville, Maryland; Ashburn, Virginia; and Silver Spring, Maryland. We conducted an exit conference with Department and FSA officials on October 20, 2017.

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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[29] Civil Rights Data Collection Reporting Web Site and Office of General Counsel Case Activity Management System.
[30] HEAL Online Processing System.
[31] IES Data Center.
[32] Individuals with Disabilities Education Act Analysis, Communication, Dissemination, and Meetings.
[33] NCES Longitudinal Studies, I3Communicty of Practice and Public Information System Website, Promise Neighborhood Website, and OSEP Personnel Development Program Data Collection System.

Enclosure 1: CyberScope FISMA Reporting Metrics

For Official Use Only

Inspector General
Section Report

2017
Annual FISMA
Report

Department of Education

For Official Use Only

For Official Use Only

Function 1: Identify - Risk Management

1 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: CA-3 and PM-5; OMB M-04-25; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4)?

Consistently Implemented (Level 3)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2017, ED-OIG/A11R0001 (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: CA-7 and CM-8; NIST SP 800-137; Federal Enterprise Architecture (FEA) Framework, v2)?

Consistently Implemented (Level 3)

Comments: 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: CA-7, CM-8, and CM-10; NIST SP 800-137; FEA Framework, v2)?

Consistently Implemented (Level 3)

Comments: 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 (NIST SP 800-53: RA-2, PM-7, and PM-11; NIST SP 800-60; CSF: ID.BE-3; and FIPS 199)?

Consistently Implemented (Level 3)

Comments: FISMA Report Issue 1. The Department's Risk Management Program Needs Improvement

For Official Use Only

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 that include 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 800-39; NIST 800-53: PM-8, PM-9; CSF: ID RM-1 – ID.RM-3; OMB A-123; CFO Council ERM Playbook)?

Consistently Implemented (Level 3)

Comments: FISMA Report Issue 1. The Department's Risk Management Program Needs Improvement

6 Has the organization defined an information security architecture and described how that architecture is integrated into and supports the organization's enterprise architecture to provide a disciplined and structured methodology for managing risk (NIST 800-39; FEA; NIST 800-53: PL-8, SA-3, and SA-8)?

Defined (Level 2)

Comments: FISMA Report Issue 1. The Department's Risk Management Program Needs Improvement

6 Has the organization defined an information security architecture and described how that architecture is integrated into and supports the organization's enterprise architecture to provide a disciplined and structured methodology for managing risk (NIST 800-39; FEA; NIST 800-53: PL-8, SA-3, and SA-8)?

Defined (Level 2)

FISMA Report Issue 1. The Department's Risk Management Program Needs Improvement

7 To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer, Chief Information Officer, Chief Information Security Officer, and other internal and external stakeholders and mission specific resources been defined and communicated across the organization (NIST 800-39: Section 2.3.1 and 2.3.2; NIST 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2, OMB A-123, CFO Council ERM Playbook)?

Defined (Level 2)

Comments: 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: CA-5; OMB M-04-25)?

Consistently Implemented (Level 3)

Comments: FISMA Report Issue 1. The Department's Risk Management Program Needs Improvement

For Official Use Only

For Official Use Only

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) selecting and implementing security controls to mitigate system-level risks (NIST 800--37; NIST 800-39; NIST 800--53: PL-2, RA-1; NIST 800-30; CSF:ID.RA-1 – 6)?

Consistently Implemented (Level 3)

Comments: 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)?

Consistently Implemented (Level 3)

Comments: FISMA Report Issue 1. The Department's Risk Management Program Needs Improvement

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 (FAR Case 2007--004; Common Security Configurations; FAR Sections: 24.104, 39.101, 39.105, 39.106, 52.239-1; President's Management Council; NIST 800-53: SA-4; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; FY 2017 CIO FISMA Metrics: 1.7, 1.8)?

Ad Hoc (Level 1)

Comments: FISMA Report Issue 1. The Department's Risk Management Program Needs Improvement

For Official Use Only

For Official Use Only

Function 1: Identify - Risk Management

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)?

Consistently Implemented (Level 3)

Comments: 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.

Consistently Implemented (Level 3)

Comments: We determined that the Department of Education's (Department) and Federal Student Aid's (FSA) Risk Management program was consistent with the Consistently Implemented level of the maturity model, which is categorized as being not effective.

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?

We found that the Department should strengthen its controls regarding risk management in the areas of (1) updating inventory guidance; (2) ensuring Federal security control compliance and access to contractor and subcontractor systems; and (3) maintaining a complete website inventory.

Calculated Maturity Level - Consistently Implemented (Level 3)

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: CM-1; SP 800-128: Section 2.4)?

Defined (Level 2)

Comments: FISMA Report Issue 2. The Department and FSA's Configuration Management Program Needs Improvement

For Official Use Only

For Official Use Only

Function 2A: Protect - Configuration Management

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 location within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contracted systems (NIST 800--128: Section 2.3.2; NIST 800--53: CM-9)?

Defined (Level 2)

Comments: 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: CM-1; NIST 800-128: 2.2.1)

Defined (Level 2)

Comments: FISMA Report Issue 2. The Department and FSA's Configuration Management Program Needs Improvement

17 To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53: CM-2, CM-8; FY 2017 CIO FISMA Metrics: 1.4, 1.5, and 2.1; CSF: ID.DE.CM-7)?

Defined (Level 2)

Comments: 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: CM-6, CM-7, and SI-2; FY 2017 CIO FISMA Metrics: 2.2; SANS/CIS Top 20 Security Controls 3.7)?

Ad Hoc (Level 1)

Comments: 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: CM-3, SI-2; NIST 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20 Control 4.5; and DHS Binding Operational Directive 15-01)?

Defined (Level 2)

Comments: FISMA Report Issue 2. The Department and FSA's Configuration Management Program Needs Improvement

For Official Use Only

Function 2A: Protect - Configuration Management

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (FY 2017 CIO Metrics: 2.26, 2.27, 2.29; OMB M-08-05)?

Consistently Implemented (Level 3)

Comments: FISMA Report Issue 2. The Department and FSA's Configuration Management Program Needs Improvement

21 To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate (NIST 800-53: CM--2, CM-3)?

Defined (Level 2)

Comments: 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?

We found that the Department (1) was not using appropriate application connection protocol; (2) was unable to protect against unauthorized devices connecting to its network; (3) used unsupported operating systems, databases, and applications in its production environment; (4) had not configured websites to encrypt data transmission; (5) failed to adequately protect personally identifiable information; and (6) along with FSA, needs to improve its controls over Web applications and servers.

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 800-53: AC-1, IA-1, PS-1; and the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

Defined (Level 2)

Comments: FISMA Report Issue 3. The Department's 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: FISMA Report Issue 3. The Department's and FSA's Identity and Access Management Program Needs Improvement

25 To what degree have ICAM policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 27 through 31) (NIST 800-53: AC-1 and IA--1; Cybersecurity Strategy and Implementation Plan (CSIP); and SANS/CIS Top 20: 14.1)?

Defined (Level 2)

Comments: FISMA Report Issue 3. The Department's 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: PS-2, PS- 3; and National Insider Threat Policy)?

Ad Hoc (Level 1)

Comments: FISMA Report Issue 3. The Department's and FSA's Identity and Access Management Program Needs Improvement

Function 2B: Protect - Identity and Access Management

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: AC-8, PL-4, and PS-6)?

Defined (Level 2)

Comments: FISMA Report Issue 3. The Department's and FSA's Identity and Access Management Program Needs Improvement

28 To what extent has the organization implemented strong authentication mechanisms (PIV or 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: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; and Cybersecurity Sprint)?

Defined (Level 2)

Comments: FISMA Report Issue 3. The Department's and FSA's Identity and Access Management Program Needs Improvement

29 To what extent has the organization implemented strong authentication mechanisms (PIV or 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: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; and Cybersecurity Sprint)?

Ad Hoc (Level 1)

Comments: FISMA Report Issue 3. The Department's and FSA's Identity and Access Management Program Needs Improvement

Function 2B: Protect - Identity and Access Management

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 2017 CIO FISMA metrics: Section 2; NIST SP 800-53: AC-1, AC-2 (2), AC-17; CSIP)?

Defined (Level 2)

Comments: FISMA Report Issue 3. The Department's 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: AC--17, SI-4; and FY 2017 CIO FISMA Metrics: Section 2)?

Defined (Level 2)

Comments: FISMA Report Issue 3. The Department's 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?

We found that the Department and FSA can strengthen their controls regarding identity and access management that will enable them to progress to the next maturity level in the areas of: (1) ensuring appropriate clearance requirements are met prior to granting system access; (2) managing external privileged accounts; (3) implementing the Identity, Credential, and Access Management strategy; (4) implementing the network access control solution; (5) displaying system warning banners; and (6) improving controls over database management.

Calculated Maturity Level - Defined (Level 2)

Function 2C: Protect - Security Training

33 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 800-53: AT-1; and NIST SP 800-50)?

Defined (Level 2)

Comments: FISMA Report Issue 4. The Department's Security Training Program Needs Improvement

34 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 800-53: AT-2 and AT-3; NIST 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181 (Draft); and CIS/SANS Top 20: 17.1)?

Defined (Level 2)

Comments: FISMA Report Issue 4. The Department's Security Training Program Needs Improvement

35 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 800--53: AT-1; NIST 800-50: Section 3))

Defined (Level 2)

Comments: FISMA Report Issue 4. The Department's Security Training Program Needs Improvement

36 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 questions 37 and 38 below) (NIST 800-53: AT-1 through AT-4; and NIST 800-50)

Defined (Level 2)

Comments: FISMA Report Issue 4. The Department's Security Training Program Needs Improvement

Function 2C: Protect - Security Training

37 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 800-53: AT-2; FY 17 CIO FISMA Metrics: 2.23; NIST 800-50: 6.2; SANS Top 20: 17.4)

Defined (Level 2)

Comments: FISMA Report Issue 4. The Department's Security Training Program Needs Improvement

38 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 800-53: AT-3 and AT-4; FY 17 CIO FISMA Metrics: 2.23)?

Defined (Level 2)

Comments: FISMA Report Issue 4. The Department's Security Training Program Needs Improvement

39.1 Please provide the assessed maturity level for the agency's Protect - Configuration Management/Identity and Access Management/Security Training (Functions 2A - 2C).

Defined (Level 2)

Comments: We determined that the Department's and FSA's configuration management programs, Identity and Access Management programs, and Security Training program were consistent with the Defined level of the maturity model. Therefore, the Protect security function was consistent with the Defined level of the maturity model, which is categorized as being not effective.

39.2 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?

Department can strengthen its controls in the area of Security Training by ensuring that contractors fulfill mandatory training requirements prior to accessing Departmental systems.

Calculated Maturity Level - Defined (Level 2)

Function 3: Detect - ISCM

40 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 organization-wide approach to ISCM (NIST SP 800-137: Sections 3.1 and 3.6)?

Defined (Level 2)

Comments: FISMA Report Issue 5. The Department's ISCM Program Needs Improvement (Repeat Finding)

41 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; collecting 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: CA-7). (Note: The overall maturity level should take into consideration the maturity of question 43)

Consistently Implemented (Level 3)

Comments: FISMA Report Issue 5. The Department's ISCM Program Needs Improvement (Repeat Finding)

42 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: CA-1; NIST SP 800-137; and FY 2017 CIO FISMA Metrics)?

Defined (Level 2)

Comments: FISMA Report Issue 5. The Department's ISCM Program Needs Improvement (Repeat Finding)

43 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: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; OMB M-14-03)?

Managed and Measurable (Level 4)

Comments: FISMA Report Issue 5. The Department's ISCM Program Needs Improvement (Repeat Finding)

Function 3: Detect - ISCM

44 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: FISMA Report Issue 5. The Department's ISCM Program Needs Improvement (Repeat Finding)

45.1 Please provide the assessed maturity level for the agency's Detect - ISCM function.

Defined (Level 2)

Comments: We determined that the Department's and FSA's ISCM programs were consistent with the Defined level of the maturity model.

45.2 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?

We found that the Department can strengthen its controls regarding ISCM that will enable it to progress to the next maturity level in the areas of (1) security control monitoring, (2) developing and identifying roles and responsibilities, and (3) fully implementing its Continuous Diagnostics and Mitigation program.

Calculated Maturity Level - Defined (Level 2)

Function 4: Respond - Incident Response

46 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: IR-1; NIST 800-61 Rev. 2; FY 2017 CIO FISMA Metrics: 4.1, 4.3, and 4.6)? (Note: The overall maturity level should take into consideration the maturity of questions 48 - -52)

Ad Hoc (Level 1)

Comments: FISMA Report Issue 6. The Department's Incident Response Program Needs Improvement (Repeat Finding)

Function 4: Respond - Incident Response

47 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; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-16-03; OMB M-16-04; FY 2017 CIO FISMA Metrics: 1.6 and 4.5; and US-CERT Federal Incident Notification Guidelines)?

Defined (Level 2)

Comments: FISMA Report Issue 6. The Department's Incident Response Program Needs Improvement (Repeat Finding)

48 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; US- CERT Incident Response Guidelines)?

Defined (Level 2)

Comments: FISMA Report Issue 6. The Department's Incident Response Program Needs Improvement (Repeat Finding)

Function 4: Respond - Incident Response

49 How mature are the organization's processes for incident handling (NIST 800-53: IR-4)?

Defined (Level 2)

Comments: FISMA Report Issue 6. The Department's Incident Response Program Needs Improvement (Repeat Finding)

50 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-16-03; NIST 800-53: IR-6; US-CERT Incident Notification Guidelines)?

Defined (Level 2)

Comments: FISMA Report Issue 6. The Department's Incident Response Program Needs Improvement (Repeat Finding)

51 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 and enter into contracts, as appropriate, for incident response support (FY 2017 CIO FISMA Metrics: 4.4; NIST SP 800-86)?

Ad Hoc (Level 1)

Comments: FISMA Report Issue 6. The Department's Incident Response Program Needs Improvement (Repeat Finding)

For Official Use Only

Function 4: Respond - Incident Response

52 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)

Defined (Level 2)

Comments: FISMA Report Issue 6. The Department's Incident Response Program Needs Improvement (Repeat Finding)

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

Defined (Level 2)

Comments: We determined that the Department' Incident Response programs were consistent with the Defined level of the maturity model.

53.2 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?

We found that the Department can strengthen its controls regarding incident response that will help enable it to progress to the next maturity level in the areas of (1) updating current guidance; (2) training key personnel; (3) the timely reporting of incidents; and (4) maintaining current interconnection security agreements.

Calculated Maturity Level - Defined (Level 2)

For Official Use Only

For Official Use Only

Function 5: Recover - Contingency Planning

54 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 800-53: CP-1 and CP-2; NIST 800-34; NIST 800-84; FCD-1: Annex B)?

Defined (Level 2)

Comments: FISMA Report Issue 7. The Department's and FSA's Contingency Planning Program Needs Improvement

55 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 56-60) (NIST SP 800-34; NIST SP 800--161).

Defined (Level 2)

Comments: FISMA Report Issue 7. The Department's and FSA's Contingency Planning Program Needs Improvement

For Official Use Only

Function 5: Recover - Contingency Planning

56 To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST 800-53: CP-2; NIST 800--34, Rev. 1, 3.2, FIPS 199, FCD--1, OMB M-17-09)?

Defined (Level 2)

Comments: FISMA Report Issue 7. The Department's and FSA's Contingency Planning Program Needs Improvement

57 To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST 800-53: CP-2; NIST 800-34)?

Defined (Level 2)

Comments: FISMA Report Issue 7. The Department's and FSA's Contingency Planning Program Needs Improvement

58 To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST 800-34; NIST 800-53: CP-3, CP-4)?

Defined (Level 2)

Comments: FISMA Report Issue 7. The Department's and FSA's Contingency Planning Program Needs Improvement

Function 5: Recover - Contingency Planning

59 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST 800--53: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD1; NIST CSF: PR.IP- 4; and NARA guidance on information systems security records)?

Consistently Implemented (Level 3)

Comments: FISMA Report Issue 7. The Department's and FSA's Contingency Planning Program Needs Improvement

60 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 800-53: CP-2, IR-4)?

Managed and Measurable (Level 4)

Comments: FISMA Report Issue 7. The Department's and FSA's Contingency Planning Program Needs Improvement

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

Defined (Level 2)

Comments: We determined that the Department's and FSA's Contingency Planning programs were consistent with the Defined level of the maturity model.

Function 5: Recover - Contingency Planning

61.2 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?

We found that the Department can strengthen its controls regarding contingency planning that will enable it to progress to the next maturity level in the areas of (1) enterprise skill assessment; (2) documenting contingency plans, business impact assessments, and contingency plan testing; and (3) contingency plan completeness.

Calculated Maturity Level - Defined (Level 2)

Function 0: Overall

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

Not Effective

Comments: We found the Department and FSA were not effective in all five security functions—Identify, Protect, Detect, Respond, and Recover.

1.2 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.

Based on the maturity model provided in the FY 2017 IG FISMA Metrics, we found the Department and FSA were not effective in all five security functions—Identify, Protect, Detect, Respond, and Recover. We also identified findings in all seven metric domains: (1) Risk Management; (2) Configuration Management; (3) Identity and Access Management; (4) Security Training; (5) Information Security Continuous Monitoring; (6) Incident Response; and (7) Contingency Planning. At the metric domains level, we determined that the Department's and FSA's program were consistent with the Defined level of the maturity in Configuration Management, Identity and Access Management, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning, while Risk Management was assessed at the Consistently Implemented level.

APPENDIX A: Maturity Model Scoring

Function 1: Identify - Risk Management

Function	Count
Ad-Hoc	1
Defined	2
Consistently Implemented	9
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)	0

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	1
Defined	6
Consistently Implemented	1
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	0

Function 2B: Protect - Identity and Access Management

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

Function 2C: Protect - Security Training

Function	Count
Ad-Hoc	0
Defined	6
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	0

Function 3: Detect - ISCM

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

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	2
Defined	5
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	0

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	0
Defined	5
Consistently Implemented	1
Managed and Measurable	1
Optimized	0
Function Rating: Defined (Level 2)	0

Maturity Levels by Function

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that the Department of Education's (Department) and Federal Student Aid's (FSA) Risk Management program was consistent with the Consistently Implemented level of the maturity model, which is categorized as being not effective.

Function 2: Protect - Configuration Management / Identity Management / Security Training	Defined (Level 2)	Defined (Level 2)	We determined that the Department and FSA's configuration management program, identity and access management program, and security training program were consistent with the Defined level of the maturity model.

Function 3: Detect - ISCM	Defined (Level 2)	Defined (Level 2)	We determined that the Department and FSA's ISCM programs were consistent with the Defined level of the maturity model.
Function 4: Respond - Incident Response	Defined (Level 2)	Defined (Level 2)	We determined that the Department and FSA's Incident Response program were consistent with the Defined level of the maturity model

Function 5: Recover - Contingency Planning	Defined (Level 2)	Defined (Level 2)	We determined that the Department and FSA's Contingency Planning programs were consistent with the Defined level of the maturity model.
Overall	Not Effective	Not Effective	

Enclosure 2: Management Comments

UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF THE CHIEF INFORMATION OFFICER

THE CHIEF INFORMATION OFFICER

DATE: October 30, 2017

TO: Charles E. Coe, Jr.
Assistant Inspector General
Information Technology Audits and Computer Crimes Investigations

FROM: Joseph C. Conaty
Delegated the Duties and Functions
Of the Deputy Secretary

Wayne Johnson
Chief Operating Officer
Financial Student Aid

SUBJECT: DRAFT Audit Report
The U.S. Department of Education's Federal Information Security Modernization Act of 2014 for Fiscal Year 2017
Control Number ED-OIG/A11R0001

Thank you for the opportunity to review and comment on the Draft Office of Inspector General's (OIG) Report, Audit of the U.S. Department of Education's Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year (FY) 2017, Control Number ED-OIG/A11R0001. The Department values the FISMA audit activity and appreciates the benefits of the collaborative relationship between the OIG and the Department, formed through years of mutual goals and objectives.

The Office of the Chief Information Officer recognizes that the objective of the OIG FISMA audit was to evaluate and determine the effectiveness of the information security program policies, procedures, and practices of the Department. As the report indicates, the Department has implemented a comprehensive set of activities to strengthen the overall cybersecurity of its networks, systems, and data as highlighted by the improvement of two Security Functions (*Detect* and *Respond*) from 'Ad-hoc' to 'Defined'.

Similar to prior year audits, the Department has garnered significant benefits from the OIG recommendations. The Department expects that the recommendations presented in this audit will further improve the effectiveness of the information security program. The Department will address each finding and recommendation in the plan provided and as agreed upon by your office.

The following responses address each recommendation:

REPORTING METRIC DOMAIN No.1: RISK MANAGEMENT

The OIG recommends that the Deputy Secretary require OCIO to:

OIG Recommendation 1.1: Incorporate additional measures to, at a minimum, achieve Level 4 status of the Risk Management program.

Management Response: The Department concurs with this recommendation. During FY 2017, the Department completed a number of actions to include all requirements of the President's Executive Order and OMB M-17-25. This effort included the completion of risk assessments for all systems in the FISMA inventory and the formal designation of a Senior Accountable Official for cybersecurity risk. The Department will continue to improve its Risk Management program and develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

OIG Recommendation 1.2: Ensure that "Information Technology Security General Support Systems and Major Applications Inventory Guidance, Version 1.0" is updated.

Management Response: The Department does not concur with this recommendation. As the report states, the Department released Information Assurance Services 02, "System Inventory Methodology and Guidance," and the Information Assurance Services 03, "System Categorization Guidance," that supersede the "Information Technology Security General Support Systems and Major Applications Inventory Guidance, Version 1.0."

OIG Recommendation 1.3: Ensure that all contracts are reviewed and re-evaluated to ensure that required access and security language is included.

Management Response: The Department concurs with this recommendation. Prior to the release of this report, the Department completed a review of nearly 200 acquisition packages to ensure that all included proper cybersecurity clauses and requirements statements. To further strengthen contractual language, the Chief Information Security Officer (CISO) is working with the Department's Contracts and Acquisition team to update contractual requirements to enforce cyber requirements for all Departmental IT acquisitions. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

OIG Recommendation 1.4: Establish a centralized tracking process for maintaining all active websites for the Department.

Management Response: The Department concurs with this recommendation. Work to resolve this finding is underway in accordance with the Department of Homeland Security (DHS) Binding Operation Directive (BOD) 18-01. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

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 will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

OIG Recommendation 2.2: Immediately correct or mitigate the vulnerabilities identified during the vulnerability assessment.

Management Response: The Department concurs with this recommendation. Once these vulnerabilities were reported by the OIG, the Department provided notification and instruction to all affected system stakeholders to immediately mitigate or resolve the vulnerability in accordance with the Department's Vulnerability and Patch Management Guidance.

OIG Recommendation 2.3: Ensure POA&Ms are created to remedy infrastructure vulnerabilities identified in the hosting data center environments.

Management Response: The Department concurs with this recommendation. Once provided with vulnerability information by the OIG, the Department notified and instructed all affected system stakeholders to open and implement Plans of Action and Milestones (POA&Ms) in accordance with the requirements identified in the Department's Vulnerability and Patch Management Guidance.

The OIG recommends that the Deputy Secretary require OCIO to:

OIG Recommendation 2.4: At a minimum, enforce TLS 1.1 or higher as the only connection for all Department connections. (Repeat Recommendation)

Management Response: The Department partially concurs with this recommendation. OCIO published the requirement to implement Transport Layer Security (TLS) version 1.1 in section *4.15.2 Policies* of the *Departmental Handbook for Information Assurance/Cybersecurity Policy (OCIO-01)*, dated January 18, 2017. As a result of the FY 2016 FISMA report and associated finding, the Department led an effort to ensure that POA&Ms and/or Risk Acceptance Forms (RAFs), as appropriate, were completed for each system that was identified to have this vulnerability. The Department will work with the OIG to validate this finding and, if required, develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

OIG Recommendation 2.5: Discontinue the use of or develop a justification for using unsupported operating systems, databases, and applications. (Repeat Recommendation)

Management Response: The Department partially concurs with this recommendation. At the time of this response, OCIO had not received the background information from the OIG to validate this finding. Some software may be listed as "unsupported" by the vendor, but there may be mitigations in place that allows the continued use of the software on the network. For example, the Program Office associated to the system may have procured additional support and maintenance from the vendor until upgrades can occur. The Department will work with the OIG to validate this finding and, if required, develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

OIG Recommendation 2.6: Ensures 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. At the time of this report, 87% of the Department's top-level domains were compliant. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

OIG Recommendation 2.7: Configure all websites to display warning banners when users login to

Departmental resources.

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

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

OIG Recommendation 2.8: Ensure that all websites and portals hosting personally identifiable information are configured not to display clear text.

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

OIG Recommendation 2.9: Eliminate the use of social security numbers as an authentication element when logging onto FSA websites by requiring the user to create a unique identifier for account authentication. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

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. During FY 2017, the Department hosted Identity, Credential, and Access Management (ICAM) Solution briefings for all Department business and system stakeholders as part of the Department's ICAM communication strategy. Further, the Department updated the ICAM Roadmap and Implementation Plan. Additionally, the Department has worked with the General Services Administration (GSA) to utilize the USAccess program to enable more efficient and secure credentialing services for Department users nationwide. The Department will continue its progress on developing the Identity and Access Management Program and will develop Corrective Action Plan by December 1, 2017 to address the associated finding.

OIG Recommendation 3.2: Ensure, in cooperation with the Office of Management, that background investigations are conducted (1) prior to granting access to Departmental and FSA systems; and (2) to ensure the correct level of access is granted.

Management Response: The Department concurs with this recommendation. During Cybersecurity Steering Committee meetings, Department officials conducted multiple sessions to assist members in clarifying background investigation requirements and processes in support of access to Department IT systems. As a result of the September meeting, the Department's Office of Management (OM) team will produce an interim guidance memo, in advance of a complete update, on the Department's personnel security, background investigations, and suitability vetting policy and processes for government staff and contractors. The Department will continue its work to resolve this finding and develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

OIG Recommendation 3.3: Prohibit contractors from granting access to FSA systems without approval by the Department.

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

OIG Recommendation 3.4: Enforce two-factor authentication is configured for all user connections to systems and/or applications housing personally identifiable information.

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

The OIG recommends that the Deputy Secretary require OCIO to:

OIG Recommendation 3.5: Ensure the Department's ICAM strategy is fully implemented to ensure that the Department meets full Federal government implementation of ICAM.

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

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. (Repeat Recommendation)

Management Response: The Department partially concurs with this recommendation. The Department completed the implementation of the network access control solution during FY 2017. During testing, the OIG discovered configuration issues. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding and configuration issue.

OIG Recommendation 3.7: Create POA&Ms to remedy database vulnerabilities for all database vulnerabilities identified.

Management Response: The Department concurs with this recommendation. Once provided with vulnerability information by the OIG, the Department notified and instructed all affected system stakeholders to open POA&Ms in accordance with the requirements identified in the Department's Vulnerability and Patch Management Guidance.

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

OIG Recommendation 3.8: Establish a process for identifying, managing, and tracking activity of privileged user accounts.

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

REPORTING METRIC DOMAIN No.4: SECURITY TRAINING

The OIG recommends that the Deputy Secretary and Chief Information Officer to:

OIG Recommendation 4.1: 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. Over FY 2017, the Department completed several deliverables to meet Cybersecurity Workforce Development objectives.

This included the coordination of the Department's response for the Federal Cybersecurity Workforce Capability Assessment, which we provided to Congress in December 2016. Other deliverables included the Department's Cybersecurity Workforce Development Strategy and Program Plan, the Cybersecurity Certification Program Guidance for ED Information Technology Professionals, and the Information Technology (IT) Cyber Security Awareness and Training Program – Tactical Plan. In addition, the Department has provided three mandatory cybersecurity training courses. The courses consist of Cyber Security and Privacy Awareness, Emailing Sensitive Personally Identifiable Information, and The Phishing Threat. In an effort to reinforce lessons learned during the training programs, the Department executed five simulated phishing exercises in FY 2017. These exercises strengthen the Department's ability to reduce risks to systems and information through modified user behavior and improved resilience to spear phishing, malware, and drive-by attacks. The Department will continue the progress made throughout FY 2017 and further develop the Department's Security Training Program by developing a Corrective Action Plan by December 1, 2017 to address the associated finding.

OIG Recommendation 4.2: Ensure that contractors fulfill mandatory training requirements prior to accessing Departmental systems.

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

REPORTING METRIC DOMAIN No.5: INFORMATION SECURITY CONTINUOUS MONITORING

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

OIG Recommendation 5.1: Incorporate additional measures to, at a minimum, achieve Level 4 Managed and Measurable status of the Information Security Continuous Monitoring (ISCM) program.

Management Response: The Department concurs with this recommendation. Over FY 2017, the Department published version 3.0 of the ISCM Roadmap that outlines the Department's strategy for maturing ISCM across the Department. To better assess and provide support for its ISCM roadmap, the Department completed a knowledge, skills, and abilities assessment that included the documentation of ISCM roles and responsibilities of ISCM stakeholders throughout the Department. The Department will continue to make progress in developing the ISCM program and will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

The OIG recommends that the Deputy Secretary and Chief Information Officer to:

OIG Recommendation 5.2: Automate its capabilities for monitoring the security controls effectiveness and overall implementation of the ISCM Roadmap.

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

OIG Recommendation 5.3: Ensure that ISCM stakeholders with designated roles and responsibilities are properly educated and engaged.

Management Response: The Department concurs with this recommendation. The Department completed the ISCM assessment in FY 2017 and provided a report on the results on January 12, 2017. The Department identified and reported a number of actions to take throughout the remainder of FY 2017

and FY 2018 to address gaps found during the assessment. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

OIG Recommendation 5.4: Ensure all Information System Security Officers have established and utilize CSAM accounts, and that required points of contacts are identified.

Management Response: The Department concurs with this recommendation. The Department reported this information to all ISSOs during quarterly Risk Management Workshops and requested that ISSOs take action to address the issue. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

OIG Recommendation 5.5: Ensure the completion of Phase 2 of the CDM program.

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

REPORTING METRIC DOMAIN No.6: INCIDENT RESPONSE

The OIG recommends that the Deputy Secretary and Chief Information Officer to:

OIG Recommendation 6.1: 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. During FY 2017, the Department's Security Operations Center (SOC) developed an Incident Response Maturity Model to measure the Department's *Detect* and *Respond* capability maturity as well as conducted a knowledge, skills, and abilities assessment in support of OMB M-16-04. To better open lines of communication between system stakeholders and incident responders, points of contact were identified for all Department/FSA systems, including all externally hosted systems. This effort facilitated timely reporting of urgent actions, such as the National Security Agency (NSA) Operational Risk Notice (ORN) and the DHS BOD. The Department will continue to improve the Department's Incident Response Program and develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

OIG Recommendation 6.2: Update OCIO Handbook-14, "Information Security Incident Response and Reporting Procedures".

Management Response: The Department partially concurs with this recommendation. While not published during the course of the audit fieldwork, the updated handbook was signed on September 27, 2017. Over FY 2017, the Department's Cybersecurity Policy Division has worked to streamline the policy creation and review processes. This effort will continue into FY 2018 to ensure that Departmental Guidance is updated in a timely manner.

OIG Recommendation 6.3: Establish a specific training curriculum for key personnel who respond to incidents when they occur.

Management Response: The Department concurs with this recommendation. During FY 2017, FSA established an initial program that allocated training based on the December Education Workforce Development Plan to all key individuals with significant security responsibilities (SSR). The training plan assigned industry-standard best-practice curricula to each person on a per-role basis. Over a hundred individuals were assigned in-depth cybersecurity training via the Department of Education learning system in industry certification preparation courses such as Security +, CISM and CISA. This program

went into effect in May of 2017. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

OIG Recommendation 6.4: Ensure that incidents are submitted to US-CERT within the required timeframe and all incidents identified as Categories 1 through 4 to the OIG that could possibly relate to cyber-fraud.

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

OIG Recommendation 6.5: Ensure that the ISA for participation in DHS' EINSTEIN program is updated and approved.

Management Response: The Department partially concurs with this recommendation. While not published during the course of the audit fieldwork, the ISA for the EINSTEIN program was updated on October 12, 2017. A copy of this document was provided to the OIG for their records.

REPORTING METRIC DOMAIN No.7: CONTINGENCY PLANNING

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

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

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

The OIG recommends that the Deputy Secretary and Chief Information Officer to:

Recommendation 7.2: Ensure that skill assessments are being measured at the enterprise level.

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

Recommendation 7.3: Ensure that contingency plans, BIAs, and results of contingency plan testing are documented in a consistent and timely manner.

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

Recommendation 7.4: Ensure that contingency plans include all required information.

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 1, 2017 to address the associated finding.

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
Dan Galik
Keith Wilson
Leslie Willoughby