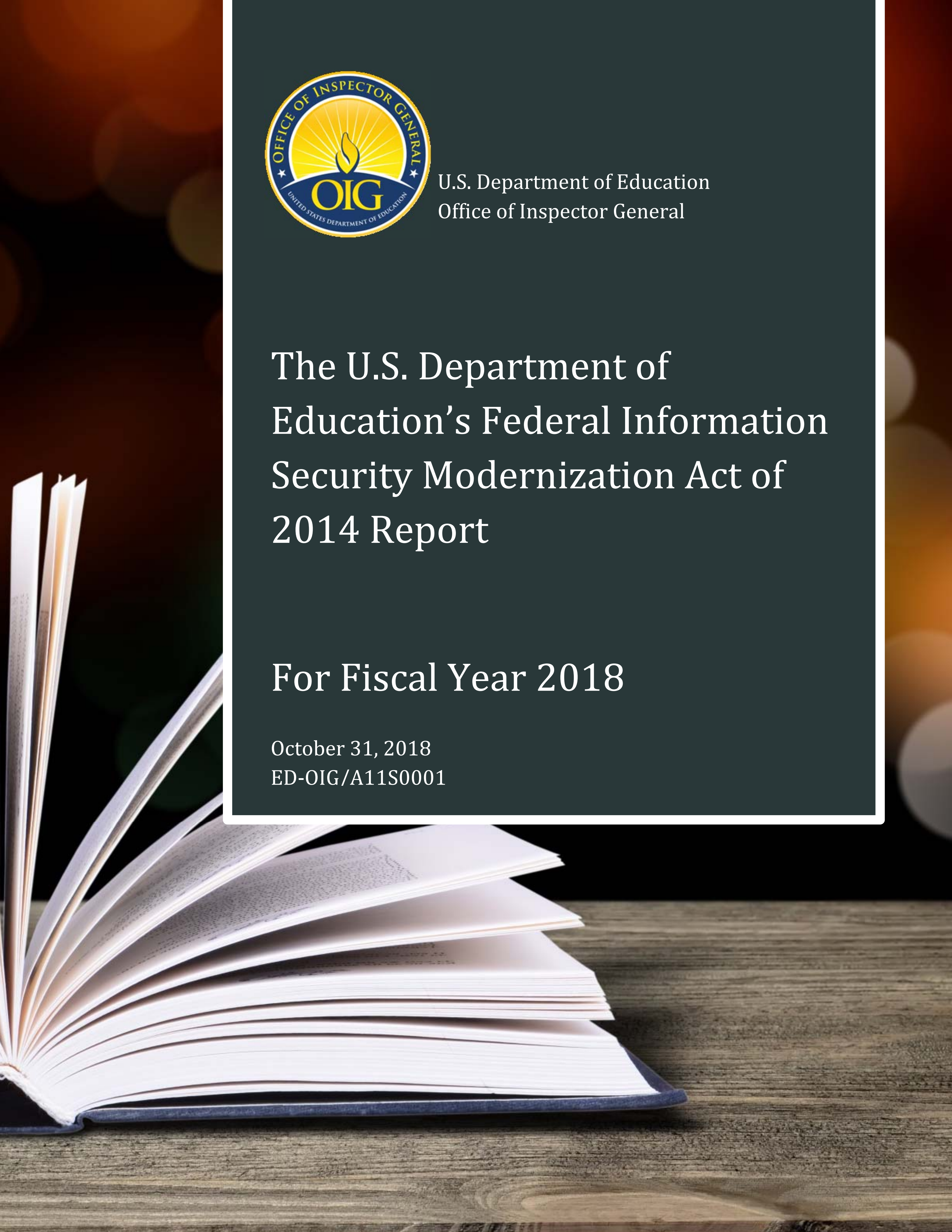


U.S. Department of Education
Office of Inspector General

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

For Fiscal Year 2018

October 31, 2018
ED-OIG/A11S0001

NOTICE

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

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

UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Information Technology Audit Division

October 31, 2018

TO: Mitchell Zais, PhD
Deputy Secretary

James Manning
Acting Chief Operating Officer

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

SUBJECT: Final Audit Report
The U.S. Department of Education's Federal Information Security Modernization Act of 2014 for Fiscal Year 2018
Control Number ED-OIG/A11S0001

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 2018. An electronic copy has been provided to your Audit Liaison Officers. We received your comments on the findings and recommendations in our draft report.

Corrective actions proposed (resolution phase) and implemented (closure phase) by your offices will be monitored and tracked through the Department's Audit Accountability and Resolution Tracking System. The Department's policy requires that you develop a final corrective action plan for our review in the automated system within 30 days of the issuance of this report. The corrective action plan should set forth the specific action items and targeted completion dates, necessary to implement final corrective actions on the findings and recommendations contained in this final audit report.

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

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

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

Enclosure

cc:

Jason Gray, Chief Information Officer, Office of the Chief Information Officer
Ann Kim, Deputy Chief Information Officer, Office of the Chief Information Officer
John Fare, Chief Information Officer, Federal Student Aid
Wanda Broadus, Acting Deputy Chief Information Officer, Federal Student Aid
Steven Hernandez, Director, Information Assurance Services, Office of the Chief Information Officer
Dan Commons, Director, Information Technology Risk Management Group, Federal Student Aid
Kelly Cline, Audit Liaison, Office of the Chief Information Officer
Stefanie Clay, Audit Liaison, Federal Student Aid
Bucky Methfessel, Senior Counsel for Information & Technology, Office of the General Counsel
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

Results in Brief

What We Did

Our objective was to determine whether the U.S. Department of Education's (Department) and Federal Student Aid's (FSA) overall information technology security programs and practices were effective as they relate to Federal information security requirements. The Fiscal Year 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics (FY 2018 IG FISMA Metrics) are grouped into five cybersecurity framework security functions that have a total of eight metric domains (as outlined in the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity):

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

Under the FY 2018 IG FISMA Metrics, inspectors general assess the effectiveness of each security function using maturity level scoring prepared in coordination with the Office of Management and Budget and the Department of Homeland Security. The five maturity level scores are outlined in the FY 2018 IG FISMA Metrics as follows: (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 our objective, we conducted audit work in the eight metric domains. We assessed the effectiveness of security controls based on the extent to which the controls were implemented correctly, operating as intended, and producing the desired outcome

[1] These functions are defined in the Background section, in the paragraph preceding Table 2.

with respect to meeting the security requirements for the information systems we reviewed in their operational environment. [2]

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 2018 IG FISMA Metrics. We report our results on each of these metric domains to the Office of Management and Budget as required; see Appendix C. 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.

What We Found

Per the FY 2018 IG FISMA Metrics, we found the Department and FSA were not effective in any of the five security functions—Identify, Protect, Detect, Respond, and Recover. We also identified findings in all eight metric domains, of which seven are repeat findings. Repeat findings are current report findings with the same or similar conditions contained in prior Office of Inspector General reports. At the metric domain levels, 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, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, and Incident Response. "Defined" means policies, procedures, and strategy are formalized and documented but not consistently implemented. We determined the programs were consistent with the maturity level of Consistently Implemented for Risk Management and Contingency Planning. "Consistently Implemented" means policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.

The Department demonstrated some improvement from fiscal year 2017 in several metric areas, most notably in contingency planning where the maturity level improved from Defined to Consistently Implemented. While the overall maturity level did not

[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."

improve for Risk Management, Configuration Management, and Incident Response, the Department did make improvement on individual metric scoring questions in each of these functions. For example, Department improved from defined to optimized for two Risk Management metric questions. Specifically, we found the Department and FSA have improved their risk management programs by implementing the Department's Cybersecurity Framework Risk Scorecard used to perform regular framework-based risk assessments, identify gaps and improvement opportunities, enhance incident response capabilities, and protect its network assets and data. The results of Cybersecurity Framework risk assessments are utilized as a mechanism to inform overall cybersecurity strategic planning at the Department-level. Listed below is a comparison of how the Department and FSA scored for fiscal years 2017 and 2018.

Table 1. Metric Domain Scoring in Fiscal Years 2017 and 2018

Metric Domain	Maturity Level 2017	Maturity Level 2018	Scores for Metric Questions 2017	Scores for Metric Questions 2018
Risk Management	Consistently Implemented	Consistently Implemented	• 8 at Consistently Implemented • 3 at Defined • 1 at Ad Hoc	• 2 at Optimized • 6 at Consistently Implemented • 3 at Defined • 1 at Ad Hoc
Configuration Management	Defined	Defined	• 1 at Consistently Implemented • 6 at Defined • 1 at Ad Hoc	• 1 at Consistently Implemented • 6 at Defined
Identity and Access Management	Defined	Defined	• 7 at Defined • 2 at Ad Hoc	• 7 at Defined • 2 at Ad Hoc
Data Protection and Privacy	Not Applicable	Defined	Not Applicable	• 5 at Defined
Security Training	Defined	Defined	• 6 at Defined	• 6 at Defined
Information Security Continuous Monitoring	Defined	Defined	• 1 at Managed and Measurable • 1 at Consistently Implemented • 3 at Defined	• 1 at Managed and Measurable • 4 at Defined

Metric Domain	Maturity Level 2017	Maturity Level 2018	Scores for Metric Questions 2017	Scores for Metric Questions 2018
Incident Response	Defined	Defined	• 5 at Defined • 2 at Ad Hoc	• 1 at Managed and Measurable • 1 at Consistently Implemented • 5 at Defined
Contingency Planning	Defined	Consistently Implemented	• 2 at Managed and Measurable • 5 at Defined	• 2 at Managed and Measurable • 3 at Consistently Implemented • 2 at Defined

Maturity Level Metric Scoring for Table 1

Level 1 = Ad Hoc
Level 2 = Defined
Level 3 = Consistently Implemented
Level 4 = Managed and Measurable
Level 5 = Optimized

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

Our answers to the questions in the FY 2018 IG FISMA Metrics template, which will become the CyberScope report, are shown in Appendix C. In addition, we have identified the current status of the Department's new cybersecurity policy framework implementation in Appendix B.

What We Recommend

We made 45 recommendations (28 of which are repeat recommendations) to assist the Department and FSA with increasing the effectiveness of their information security programs. This will help the Department and FSA fully comply with all applicable requirements of FISMA, the Office of Management and Budget, the Department of Homeland Security, and the National Institute of Standards and Technology.

The Department concurred with 39 recommendations, partially concurred with 4 recommendations, and did not concur with 2 recommendations. We summarized and responded to specific comments in the "Audit Results and Findings" section of the report. We considered the Department's comments, but did not revise our findings and recommendations.

Introduction

Purpose

We performed this audit based on requirements specified by the Federal Information Security Modernization Act of 2014 (FISMA) and the Fiscal Year 2018 Inspector General FISMA Metrics V1.0.1 (FY 2018 IG FISMA Metrics), May 24, 2018. Our audit focused on reviewing the five security functions and eight associated metric domains: Identify (Risk Management), Protect (Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training), Detect (Information Security Continuous Monitoring), Respond (Incident Response), and Recover (Contingency Planning).

Background

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

The E-Government Act also assigned specific responsibilities to the Office of Management and Budget (OMB), agency heads, chief information officers, and inspectors general. It established that OMB is responsible for creating and overseeing policies, standards, and guidelines for information security and has the authority to approve agencies' information security programs. OMB is also responsible for submitting the annual Federal Information Security Management Act of 2002 report to Congress, developing and approving the cybersecurity portions of the President's Budget, and overseeing budgetary and fiscal issues related to the agencies' use of funds.

Each agency must establish a risk-based information security program that ensures information security is practiced throughout the life cycle of each agency's systems. Specifically, the agency's chief information officer is required to oversee the program, which must include the following:

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

In December 2014, FISMA, was enacted to update the Federal Information Security Management Act of 2002 by (1) reestablishing the oversight authority of the Director of OMB with respect to agency information security policies and practices and (2) setting forth authority for the Department of Homeland Security (DHS) Secretary to administer the implementation of such policies and practices for information systems.

FISMA requires the Office of Inspector General (OIG) to assess the effectiveness of the agency's information security program. FISMA specifically mandates that each evaluation under this section must include (1) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems and (2) an assessment of the effectiveness of the information security policies, procedures, and practices of the agency.

The Council of the Inspectors General on Integrity and Efficiency, OMB, and DHS developed the FY 2018 IG FISMA Metrics, in consultation with the Federal Chief Information Officer Council. The FY 2018 IG FISMA Metrics are organized around the five information Cybersecurity Framework security functions outlined in the NIST's "Framework for Improving Critical Infrastructure Cybersecurity," as shown in Table 2. [3]

Table 2. Aligning the Security Functions to the FY 2018 IG FISMA Metric Domains

Security Functions	FY 2018 IG Metric Domains
Identify	Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

FISMA and the FY 2018 IG FISMA Metrics require the inspectors general to assess the effectiveness of information security programs on a maturity model spectrum, in which the foundation levels ensure that agencies develop sound policies and procedures and the advanced levels capture the extent to which agencies institutionalize those policies and procedures. Table 3 details the five maturity model levels: (1) Ad Hoc, (2) Defined, (3) Consistently Implemented, (4) Managed and Measurable, and (5) Optimized. Within the context of the maturity model, Levels 4 or 5 represent an effective level of security.[4]

[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.

[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.

Table 3. 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 2018 IG FISMA Metrics, ratings throughout the eight domains are by simple majority. Further, Inspectors General determine the overall agency rating and the rating for each of the Cybersecurity Framework Functions at the maturity level.

Beginning in fiscal year (FY) 2009, OMB required Federal agencies and OIGs to submit FISMA reporting through the OMB Web portal, CyberScope (Appendix C).

Departmental Systems and Security Program Description

In September 2007, the Department replaced its enterprise-wide network and information technology support services contract with the Education Department Utility for Communications, Applications, and Technology Environment contract (EDUCATE). Supporting 6,100 end-users nationwide, EDUCATE was a 10-year performance-based contract that moved the Department to a contractor-owned, contractor operated infrastructure service model for managing information technology. The EDUCATE contract's final option year ended in November 2017.

The Department's Information Technology Service's Re-Compete initiative established the Portfolio of Integrated Value-Oriented Technologies (PIVOT) that awarded services to vendors based on a multi-contract acquisition approach. This approach is designed to encourage and incentivize service providers to focus on high-quality customer service, new product innovation, flexibility in addressing new and changing requirements, and optimized cost versus benefit in the delivery of information technology services to the Department over the life of the contracts. The operational framework of the PIVOT structure includes (1) IT services oversight, (2) prime integrator and end-user services, (3) hosting, (4) mobile devices, (5) printers, and (6) network. The Department has awarded four of the contracts[5] and is in the process of awarding the remaining two.

The Federal Student Aid's (FSA) Virtual Data Center contract with Dell Services Federal Group for a general support system to consolidate and operate many of its student financial aid program systems expired in August 2016. In 2014, FSA developed a high-level strategy resulting in three service delivery models: (1) a hybrid cloud (combination of public and private cloud); (2) implementation of a contractor-owned, contractor-operated data center facility for legacy systems; and (3) mainframe operations. As a result, an 11-year contract was awarded to Hewlett-Packard Enterprises Services who proposed the Next Generation Data Center, located at its Mid-Atlantic data center in Clarksville, Virginia, and recovery site located in Colorado Springs, Colorado. These solutions (1) aim to meet NIST and FISMA security controls; (2) are monitored and managed through a single operations portal; (3) provide real-time operations visibility from application to infrastructure to security; and (4) propose an applications-focused optimization for mainframe, traditional hosting, and hybrid cloud solution. The Mid-Atlantic Data Center is managed by DCX Technologies (a sub-contractor to Hewlett-Packard). The transition from the Virtual Data Center to Next Generation Data Center occurred in phases during 2017 through migration waves. This began with establishing an Authorization to Operate for the Next Generation Data Center general support system, and followed with separate migration waves that included the (1) Foundation Wave, (2) SharePoint Wave, (3) Integrated Technical Architecture Wave, (4) Financial Management Service operations, (5) Free Application for Federal Student Aid Wave, and (6) ez-Audit, Postsecondary Educational Participant System, and eApp operations. The decommissioning of the Virtual Data Center site began in May 2018.

[5] Includes the contracts for oversight, printers, mobile devices(which will be re-competed in the fall of 2018), and the network.

The Department's total spending for IT investments for the FY 2018 was estimated at about $707 million.

Through the Office of the Chief Information Officer (OCIO), the Department monitors and evaluates the contractor-provided information technology services through a service-level agreement framework and develops and maintains common business solutions that are required by multiple program offices. OCIO advises and assists the Secretary and other senior officials to ensure that the Department acquires and manages information technology resources in a manner that is consistent with the requirements of the Clinger-Cohen Act of 1996,[6] FISMA, and OMB Memorandum A-130.[7] OCIO is responsible for implementing the operative principles established by legislation and regulation, establishing a management framework to improve the planning and control of information technology investments, and leading change to improve the efficiency and effectiveness of the Department's operations. In addition to OCIO, FSA has its own chief information officer, whose primary responsibility is to promote the effective use of technology to achieve FSA's strategic objectives through sound technology planning and investments, integrated technology architectures and standards, effective systems development and production support. FSA's Chief Information Officer core business functions include the (1) Application Development Group, (2) Enterprise IT Management Group, and (3) Enterprise IT Services Group.

Fiscal Year 2017 FISMA Audit Results

During last year's FISMA audit, we identified 7 findings and provided 35 recommendations that addressed the conditions noted in the report. The Department concurred with 31 recommendations, partially concurred with 3, and did not concur with 1. It also provided corrective action plans on how it would address the recommendations. In general, our findings identified:

- outdated policies and procedures;
- unauthorized and unsecure connections to the Department's network;
- reliance on unsupported systems, databases, and applications;

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

[7] 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.

- privileged system user accounts not properly managed;
- personally identifiable information not being protected;
- external network connections not using two-factor authentication;
- insufficient implementation of a network access control solution;
- an insufficiently implemented information security continuous monitoring program; and
- an insufficiently implemented incident response program.

The Department and FSA agreed to corrective actions such as reviewing acquisition packages for cybersecurity requirements and causes, providing immediate notification to stakeholders to mitigate and resolve identified vulnerabilities, updating policies and procedures, updating Identity, Credential, and Access Management (ICAM) Roadmap and Implementation Plan, establishing cybersecurity workforce development documents, communicating issues through Risk Management Workshops, and developing an Incident Response Maturity Model. As of August 2018, the Department and FSA reported that they had completed corrective actions for 15 of the 35 recommendations. The Department and FSA anticipate completing a majority of the corrective actions by October 31, 2018, with some extending out as far as July 2019.

Audit Results and Findings

We identified findings in all eight metric domains. Our findings in these metric domains included repeat findings with same or similar conditions from OIG reports issued from FYs 2011 through 2017.

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 Level 3: Consistently Implemented level of the maturity model, which is categorized as being not effective. We found the Department and FSA (1) established policies and procedures consistent with NIST standards; (2) maintained an enterprise architecture that includes security of components; (3) relied on a Department-wide Risk Management Framework; (4) used an enterprise-wide Cybersecurity Framework Risk Scorecard; (5) established a Plan of Action and Milestones (corrective action plan) process to identify, track, and remediate weaknesses; and (6) established workshops and forums to inform stakeholders on risk management issues. However, we noted some improvements are needed in the Department and FSA’s (1) corrective action plan remediation process, and (2) enforcing and monitoring inclusion of the required contract clauses.

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 corrective action plan is a management tool for tracking the mitigation of cybersecurity program and system-level findings and weaknesses. The purpose of a corrective action plan is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

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. We also identified areas where the Department and FSA continue to develop and strengthen its risk management program. For instance, in August 2017, it implemented its Cybersecurity Framework Risk Scorecard that communicates the Department’s risks to all stakeholders and is used to perform regular framework-based risk assessments. However, while the Department has made improvements to its risk management program, its practices in 10 of the 12 areas still do not meet Managed and Measurable or an effective level of security. The Department would need to achieve an effective level of security for at least 7 of the 12 metric questions. For example, the Department would need to ensure that the information systems included in its inventory are subject to the monitoring processes defined within the organization's Information Security Continuous Monitoring (ISCM) strategy.

We found that policies, procedures, roles, and responsibilities for system level risk assessment and security control selections, were established and communicated across the organization. Also, each principal office that owns a FISMA-reporting information system was required to provide input to the OCIO that is included in the quarterly and annual Department-wide FISMA report.

The Department and FSA rely on the Cyber Security Assessment and Management tool, as the official system of record for system documentation, and inventory of all Department and FSA systems. The use of the Cyber Security Assessment and Management tool is defined in detail in the Cyber Security Assessment and Management standard operating procedures, the Life Cycle Management Framework, and within the overarching Department cybersecurity guidance. The tool also incorporates the Risk Management Framework to provide system owners and other shareholders with the capabilities of addressing all six steps of the Risk Management Framework (including categorization and monitoring).

OCIO, in coordination with the principal offices, established and maintained an enterprise architecture that includes security for the Department’s network components. Departmental information systems are required to establish baseline security requirements in compliance with policy and Federal cybersecurity regulations. Security architecture reviews are to be conducted annually.

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

The Department’s overarching risk management strategy is documented in the Department’s Enterprise Risk Management program. As part of its risk management process, the Department also coordinates with the Cyber Risk Council and includes the Chief Financial Officer/Risk Officer in developing an overall risk strategy. In addition, FSA provides input into prioritizing enterprise-wide cyber risk. The Department also established a Risk Management Council with the goal to ensure that its risk strategy is implemented across the FSA enterprise. We also found that the Cybersecurity

Framework Risk Scorecard is aligned with the risk identified in the Enterprise Risk Management program.

The Department established a Lifecycle Management framework that provides a structured approach for managing information technology projects. The principal office that develops or procures the information system is responsible for implementing the framework for that system.

The Department relies on DHS’ Continuous Diagnostics and Mitigation program to identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. DHS approved the Department for early engagement in Phase 4 of the Continuous Diagnostics and Mitigation program. Phase 4 capabilities support the overall program goal to identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

The Department uses meetings, workshops, and monthly Cybersecurity Framework Scorecards to communicate risks by informing overall cybersecurity strategic planning at the Department level enabling strategic planners to view, understand, and manage cybersecurity risk. It also helps internal and external stakeholders to align cybersecurity activities with business requirements, risk tolerance, and resources. This was demonstrated through the Department’s Quarterly Cybersecurity Risk Management workshops, the FY 2018 Cybersecurity Forums, and distribution of the Cybersecurity Framework Scorecard to stakeholders.

The Department’s ISCM strategy captures its inventory monitoring and includes hardware assets and High Value Assets. The Department reviews and updates inventory at least annually, and sometimes quarterly. The Department maintains its inventory of hardware assets through the use of a Configuration Management Plan template. The ISCM Strategy also addresses the responsibility for maintaining information technology assets and managing software.

The Department has a process to track its corrective action plans for security weaknesses, and it maintains and tracks these plans using the Cyber Security Assessment and Management tool. This includes the centralized tracking of security weaknesses, prioritization of remediation efforts, maintenance, and independent validation of corrective action plans. The Cyber Security Assessment and Management tool provides the capability to automatically notify responsible parties (i.e., system owner, Information System Security Officer, Authorizing Official) to alert them of upcoming corrective action plan milestone due dates. The system owner and Information System Security Officer must monitor corrective action plan progress. The

Department uses an independent verification and validation process to ensure that corrective action plan milestones are monitored and tracked to completion.

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

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

We found that for the Risk Management metric domain, the Department and FSA were at the Optimized level for 2 metric questions, the Consistently Implemented level for 6 metric questions, the Defined level for 3 metric questions, and the Ad Hoc level for 1 metric question. The Department and FSA should strengthen their controls regarding risk management in the areas of their (1) corrective action plan remediation process, and (2) process over monitoring and enforcing the required contract clauses.

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

The Department and FSA did not provide effective oversight of their corrective action plan remediation process. We identified a total of 18,714 corrective action plans from 2009 through 2018 in active or remediated status in the Cyber Security Assessment and Management tool. For these 18,714 corrective action plans, we found that (1) 6,397 were not assigned to an Information System Security Officer (ISSO) (2,602 attributed to FSA and 3,795 to the Department); (2) 18,162 did not have a remediation cost associated with the weakness identified; and (3) 716 had a remediation start date marked "TBD" indicating that Authorizing Officials have not started to work on resolving the weaknesses.

The Handbook for Information Assurance Cyber Security Policy defines remediation timeline requirements for criticality as being (1) within 24 hours for high vulnerabilities; (2) within 72 hours for critical security findings; (3) 7 days for high risk findings; (4) 21 days for moderate risk findings; and (5) 30 days for low risk findings. In May 2018, we identified nine FSA corrective actions for high vulnerabilities; per policy, these were required to be resolved within 24 hours. However, as of June 2018, all nine vulnerabilities remained unresolved.

Although the Department requires that corrective action plans be resolved within a year, we identified a trend that the average timeframe for remediating weaknesses is increasing. For instance, in June 2018, the Department and FSA had 3,086 open corrective action plans—with some corrective action plans dating back to 2016. In 2009, FSA's most efficient year for remediating corrective action plans, it took an average of 31 days to complete a corrective action plan. In 2018, FSA averaged

221 days. Similarly, in 2012, the Department's most efficient year for remediating corrective action plans, it took an average of 78 days to complete a corrective action plan. In 2018, the Department averaged 282 days.

NIST Special Publication (SP) 800-53, Revision 4, requires agencies to update existing corrective action plans on the organization-defined frequency based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. It further requires organizations to employ automated mechanisms to help ensure that the plan of action and milestones for the information system is accurate, up to date, and readily available. The corrective action plan process is also part of the Department's Risk Management Framework strategy's Monitor Risk Factors, where it is required to coordinate with Information System Security Officers to work corrective action plan action items and completion dates in an authorization decision. Incomplete or missing information on corrective action plans in the Cyber Security Assessment and Management tool could limit Information System Security Officers' abilities to assess system risk, evaluate funding requirements, and ensure adequate security of the systems is enforced.

Department and FSA's Process Over Monitoring Contract Clauses Needed Improvement

The Department and FSA did not have a consistent process to enforce and monitor inclusion of required contract clauses. As required by the FY 2018 IG FISMA Metrics, the Department should ensure that specific contracting language, such as appropriate information security, privacy requirements, and material disclosures; Federal Acquisition Regulation clauses; and clauses on protection, detection, and reporting of information, as well as service level agreements, are included in contracts to mitigate and monitor the risk related to contractor systems and services. We reviewed 13 contracts for our 8 judgmentally selected systems (one system had 5 contracts) to determine the extent to which the Department and FSA ensured that contracts contained specific language, including (1) privacy requirements and material disclosures, (2) standard Federal Acquisition Regulation clauses, (3) Federal Risk and Authorization Management Program standard clauses, and (4) Cloud Computing Contract Best Practices. We also determined whether the contracts contained the general access clause that would allow the Department access to contractor/subcontractor systems and whether contracts included at least the minimum security language. Out of the 12 contracts reviewed, we found that:

- 10 contracts did not include Federal Acquisition Regulation privacy clauses 52.224-1 and 52.224-2 requiring compliance with the Privacy Act;
- 11 contracts did not include Federal Acquisition Regulation clause 52.239, "Privacy or Security Safeguards," requiring contractors not to disclose security

safeguards, to provide access to the Department, and to immediately alert the Department to new threats, hazards, or non-functioning safeguards;

- 3 of the 4 contracts issued on or after the August 9, 2016, did not include the clause required by Acquisition Alert 2016-07, “Class Deviation to Implement Policy Regarding Access to Contractor Information Systems,” issued by the Office of the Chief Information Officer; and
- 3 contracts did not have required security clauses or at least minimum security language.

We reported similar conditions in our FY 2017 FISMA audit. As a result, the Department informed us that it developed an information technology Program Services review process for reviewing contacts and clauses, where every contract is reviewed to identify pertinent clauses from different perspectives (cybersecurity and architecture). Although the Department has developed this process, it was not consistently implemented as identified by the conditions noted above. [8]

Unless standard privacy, security and access clauses and provisions are included in its service contracts, the Department cannot ensure that contractors will have the necessary controls and enable the Department and the OIG to have access to contractor systems to perform necessary quality assurance, audits, and investigations.

Recommendations

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

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

1.2 Ensure the completeness of individual corrective action plans for elements including remediation officials assigned, costs associated to remediate the weakness, and starting dates to remediate the weakness.

1.3 Ensure that all contracts are reviewed and include all applicable privacy, security, and access provisions. (Repeat Recommendation)

[8] On August 16, 2018, the Department revised the completion date to January 19, 2019, and informed us that it is working with Acquisitions to ensure all contracts have the appropriate language.

Management Comments

The Department concurred with recommendations 1.1 and 1.2, and partially concurred with recommendation 1.3. For recommendations 1.1 and 1.2, the Department will develop corrective action plans by December 31, 2018 to address the associated finding.

For recommendation 1.3, the Department stated that it has developed a number of processes to review Statements of Work for proper contract language to include the OCIO Statement of Work review process and the FSA Information Resource Program Elements process. It further stated that if the contract included in the scope of the Inspector General's review occurred after the establishment of these processes, the Department will review the Statement of Work processes to ensure the contract clauses identified in the Inspector General's report are included. The Department also stated that is does not intend to review contracts executed prior to the establishment of these processes. The Department will develop a corrective action plan by December 31, 2018 to address the finding.

OIG Response

OIG will review the corrective action plans to determine if the actions will address the finding and recommendations and if so, will validated during our FY 2019 FISMA audit fieldwork.

OIG does not agree with the exclusion of contracts prior to the establishment of these processes. Without the inclusion of standard privacy, security and access clauses in all of its service contracts, the Department cannot ensure that that all contractor systems have the necessary security controls in place, and that OIG has access to these systems for quality assurance, audits, and investigative purposes.

SECURITY FUNCTION 2—PROTECT

The "Protect" security function comprises the Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training metric domains. Based on our evaluation of the four program areas, we determined that the Protect security function was consistent with the Defined level of the maturity model, which is categorized as being not effective.

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. We found that the Department and FSA employ a number of scanning tools in their assessment of potential vulnerabilities on their networks. The Department established mechanisms for disseminating information on evolving cyber threats. The Department also established an Enterprise Architecture Review Board for governance of the Department's enterprise architecture. However, the Department's practices in several areas still do not meet the Managed and Measurable threshold under the metrics to be considered effective. To achieve an effective level of security, the Department needs to achieve an effective level for at least five of the eight metric questions. For example, the Department needs to ensure that all systems required to transverse through a trusted internet connection are configured accordingly, and that all obsolete systems are retired and replaced by a new solution.

The Department's primary configuration management policy is identified in the "Handbook for Information Assurance Cybersecurity Policy." It also uses the "Information Technology Security-Focused Baseline Configuration Management Guidance, Version 1.0" to ensure compliance with basic applicable system configuration requirements and assists principal offices with the necessary security concepts in order to manage and maintain security baseline configurations.

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

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

Both the Department and FSA maintain a configuration management database of all hardware and assets that enables them to help define their security posture. Also, we verified that the Department and FSA are tracking connection security of their external facing websites.

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

OCIO established an Enterprise Architecture Review Board for governance of the Department's enterprise architecture. We verified that system changes are being submitted to the Enterprise Architecture Review Board for review by obtaining a listing of all changes submitted from July 2017 to December 2017.

Finding 2. The Department and FSA's Configuration Management Program Needs Improvement (Repeat Finding)

We found that for the Configuration Management metric domain, the Department and FSA were at the Defined level for seven metric questions and the Consistently Implemented level for one metric question. The Department and/or FSA (1) were not consistently ensuring the use of secure connections; (2) were not using appropriate application connection protocols; (3) relied on unsupported operating systems, databases, and applications in its production environment; (4) did not adequately protect personally identifiable information; (5) needed to improve their controls over web applications and servers; and (6) were not consistently performing system patching.

Department Was Not Consistently Ensuring the Use of Secure Connections

The Department was not consistently ensuring that websites are configured to use a trusted internet connection or managed trusted internet protocol services. We identified 60 systems that were required to use trusted internet connections as part of their processes. We found that only 20 (or 33 percent) of the systems are configured to use a trusted internet connection or managed trusted internet protocol services solution as required by DHS and OMB requirements. The Department will need to ensure that systems are routed through a secure connection to safeguard student information and avoid a risk of compromise.

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

31, 2016.[9] Through the use of secure connections, the Department can ensure that data transmissions are protected and decrease the risk of compromise.

Department and FSA Were Not Using Appropriate Application Connection Protocols

We found that the Department and FSA continue to use outdated secure connection protocols. Specifically, we identified that 2 out of 142 authorized connections used Transport Layer Security 1.0. In addition, based on information OCIO provided, we determined that of the 661 sites in the Department and FSA's inventory, 266 continue to use Transport Layer Security 1.0 and 1.1 as an alternate way to connect. NIST required agencies to develop migration plans to support Transport Layer Security 1.2 by January 1, 2015. We reported a similar condition in our FY 2015, 2016, and 2017 FISMA audits. However, the Department and FSA are making progress in transitioning all sites to Transport Layer Security 1.2 and above by establishing a tracking mechanism to identify sites that still do not meet the requirement. Until the Department and FSA ensure that all secure connections adhere to the required protocols, users could still expose systems to a number of vulnerabilities and exploits, including man-in-the-middle attacks that could jeopardize Department resources.[10]

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

We found that FSA still relied on a number of systems and applications that were not supported by the vendors. In addition, we found that a number of obsolete systems allowed connections to servers and network resources without requiring users to authenticate using two-factor authentication and these systems did not display login warning banners. Although Risk Acceptance Forms were in place to continue use of unsupported operating systems, databases, and applications, continued use will make these information technology solutions vulnerable to compromise. FSA stated that the current migration plan to move these systems to a new data center environment will help retire and discontinue the use of the unsupported systems. Relying on unsupported operating systems, databases, and applications, could lead to data leakage and exposure of personally identifiable information that can compromise the

[9] 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.

[10] 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.

Department’s integrity and reputation. We reported similar conditions in our FY 2015 and 2017 FISMA audits.

In addition, during our database vulnerability assessment of one of the systems, the Postsecondary Education Participants System, we were not able to perform vulnerability scans on the operating system and database because both of these system components were obsolete and could not support our scanning tool. We confirmed the obsolescence and the inability to support the scanning tool during our technical discussions with FSA personnel. Because we were not able to scan the operating system and database, we could not assess what vulnerabilities existed on these system components so that they could be remediated. As a result, these components remain vulnerable to compromise.

Personally Identifiable Information Not Consistently Protected

FSA was not ensuring that all websites mask personally identifiable information—primarily Social Security numbers—that users enter on the sites. Further, FSA continued to use Social Security numbers as an identifier on one website. Specifically, of the 653 websites we reviewed, two were not configured to mask sensitive personally identifiable information (including Social Security numbers and birth dates) and instead displayed the information in plain text as it was entered; one of these two sites used a Social Security number as a primary identifier. A user with malware on his or her system that captures screenshots could become a victim of identity theft via screen capture of the requested personally identifiable information. We have reported a similar condition relating to using Social Security numbers as a primary identifier in our FY 2014 and FY 2017 FISMA audits.

The Department’s and FSA’s Controls over Web Applications and Servers Need Improvement

We assessed web application and server vulnerability for seven of the eight judgmentally selected systems.[11] We found that the Department and FSA should improve 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, we found that although some key controls were effectively implemented (such as data validation, secure coding, and web security), the security architecture could use further enhancements to strengthen the Department’s overall security posture. For example,

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

we identified instances of (1) SQL injection execution vulnerabilities, (2) cross-site scripting, (3) cross-site forgery, (4) outdated software and systems, (5) cookie weaknesses, (6) missing patches, (7) systems running unnecessary or insecure services, (8) local administrator password was the same on multiple servers, (9) clickjacking[12], (10) running an outdated version of Drupal[13], and (11) file uploads not being scanned by antivirus software. Inadequate system configuration practices increase the potential for unauthorized activities to occur without being detected and could lead to potential theft, destruction, or misuse of Department data and its resources. We reported similar conditions in our FY 2017 FISMA audit.

FSA System Patching Was Not Consistently Performed

We found that FSA was not consistently applying software patches and security updates to its systems and information technology solutions. Most notably, some of the systems that had issues were obsolete systems. More specifically, we identified instances where critical patch updates and security updates were not being applied, as well as information technology solutions that were vulnerable to zero-day exploits. Failure to patch systems (in particular zero-day exploits) could allow a malicious user to gain access to a system and user accounts, leading to identity theft or fraud. We reported similar conditions in our FY 2015 and FY 2017 FISMA audits.

NIST SP 800-53, Revision 4, provides guidelines for selecting and specifying security controls for organization and information systems supporting the executive agencies of the Federal Government to meet the requirements of Federal Information Processing Standards Publication 200, "Minimum Security Requirement for Federal Information Systems." This includes (1) baseline configuration, (2) minimization of personally identifiable information, (3) unsupported system components, and (4) transmission confidentiality and integrity.[14] NIST SP 800-52, "Guidelines for the Selection, Configuration and Use of Transport Layer Security Implementations," states that Transport Layer Security version 1.1 is required, at a minimum, to mitigate various attacks on version 1.0 of the Transport Layer Security protocol. Support for Transport Layer Security version 1.2 is strongly recommended and agencies are required to develop migration plans to support Transport Layer Security 1.2 by January 1, 2015. NIST SP 800-46, Revision 1, "Guide to Enterprise Telework and Remote Access Security,"

[12] Allows an attacker to use transparent or opaque layers to trick a user into clicking on buttons or other controls to change operations.

[13] Content management software used for making websites and applications.

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

states that organizations should consider the use of network access control solutions that verify the security posture of a client before allowing these on an internal network.

Recommendations

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

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

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

We recommend that the Deputy Secretary require OCIO to—

2.3 Ensure that the configuration of 40 websites to be routed through a trusted internet connection or managed trusted internet protocol service.

2.4 Ensure that all existing websites and services are accessible through a secure connection as required by OMB M-15-13. (Repeat Recommendation)

We recommend that the Chief Operating Officer require FSA to—

2.5 Discontinue the use of unsupported operating systems, databases, and applications. (Repeat Recommendation)

2.6 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)

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

2.8 Immediately correct or mitigate the vulnerabilities identified during the vulnerability assessment. (Repeat Recommendation)

Management Comments

The Department concurred with the recommendations and stated it will develop corrective action plans by December 31, 2018 to address the associated finding.

OIG Response

OIG will review the corrective action plans to determine if the actions will address the finding and recommendations and if so, will validate during our FY 2019 FISMA audit fieldwork.

METRIC DOMAIN 3—IDENTITY AND ACCESS MANAGEMENT

Identity and access management refers to 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 established the "Identity, Credential, and Access Enterprise Roadmap, Version 2.0." In addition, ICAM requirements were identified as part of the new PIVOT contract for network services. Furthermore, the Department uses CyberArk Privileged Account Security to manage the access and activities of privileged users. 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 achieve an effective level of security, the Department would need to achieve that level on at least 5 of the 9 metric questions. For example, the Department would need transition to its desired or "to-be" ICAM architecture and integrate its ICAM strategy and activities with its enterprise architecture and the Federal Identity, Credentialing and Access Management segment architecture.

We found that the Department established identity and access management policies, procedures, and guidance that comply with NIST and OMB standards.

In June 2018, the Department also established an ICAM program charter that established program authority to improve coordination, management, and oversight for the realization of the Federal ICAM program within the Department. The program also helps increase security, enforce compliance with laws and regulations, improve operability, enhance customer service, eliminate redundancy, and increase protection of personally identifiable information.

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

The Department uses CyberArk Privileged Account Security system to manage the access and activities of privileged users. CyberArk manages access and activities of users with elevated privileges to information technology resources that include servers, network devices, desktop and laptops, databases, and appliances.

We judgmentally selected 10 FSA privileged users to determine whether the Department required background checks before it granted system access. For all 10 FSA privileged users, we found that the background checks were completed before granting system access.

Finding 3. The Department's and FSA's Identity and Access Management Program Needs Improvement (Repeat Finding)

We found that for the Identity and Access Management metric domain, the Department and FSA were at the Defined level for seven metric questions, and Ad Hoc level for two metric questions. The Department and FSA can strengthen their controls regarding identity and access management to enable them to progress to the next maturity level by (1) ensuring personnel security and background investigation requirement guidance is completed, (2) implementing the ICAM strategy, (3) implementing a process to manage privileged accounts, (4) consistently documenting position risk descriptions for background investigations, (5) not allowing devices to reconnect after being blocked by the Network Access Control solution, (6) fully implementing two-factor authentication; (7) consistently documenting access agreements before granting access to systems, (8) removing access of terminated users to the Department's network, (9) configuring websites to display warning banners, (10) improving controls over database management, and (11) ensuring virtual private network connections disconnect after 30 minutes of inactivity.

Personnel Security and Background Investigation Requirements Guidance Was Not Completed

In response to our FY 2017 FISMA findings to ensure that background investigations were completed before accessing systems and correct level of access is granted, the Department established corrective action plans to issue interim guidance memorandum and update Departmental Directive OM: 5-101, "Personnel Security Screening Requirements for Contractor Employees." However, we found that neither corrective action plan had been completed. The Department had extended its corrective action date for OM: 5-101 for completion in early 2019. Allowing users without proper clearance to access its systems and resources increases the risk of unauthorized access to malicious users and compromise Departmental information resources.[15]

ICAM Strategy Was Not Fully Implemented

During our FY 2017 FISMA audit, we reported that the Department was in the process of creating its ICAM structure and expected to have full Federal implementation of ICAM by the end of FY 2018. During our FY 2018 FISMA audit, we found that its ICAM implementation was not fully implemented and was scheduled for completion by October 31, 2018. The Department stated that awarding the PIVOT contracts would ensure that an Enterprise ICAM solution would be implemented to meet Federal requirements. However, the Department stated that due to the current PIVOT contract dispute, full implementation of its ICAM strategy was delayed. Without full implementation of the ICAM strategy, the Department cannot ensure its full accountability of its access management systems, especially those hosted externally. The Department's FISMA inventory consists of 132 reportable systems of which 85 are hosted at various external contractor sites, to include a number of Federal Risk and Authorization Management Program (i.e., FedRAMP) cloud service provider locations. These include several of the Department's High Value Asset systems, which are applications and systems that directly support mission essential functions.

Process to Manage Privileged Accounts Was Not Fully Implemented

We found that FSA had not fully implemented a process for identifying, managing, or tracking activity of privileged accounts. We reported this condition during our FY 2017

[15] See OIG report "The Department's Implementation of Contractor Personnel Security Clearance Process" (ED-OIG/A19P0008), September 20, 2018.

FISMA audit. As part of its corrective action plan, the Department planned to implement a process to manage and track activity of privileged users by October 31, 2018. In August 2018, we confirmed that the planned implementation of this process had been extended to January 31, 2019. In addition, scanning results of FSA servers identified access and password deficiencies associated with privileged user accounts. For example, we identified incidents of (1) an unused administrator account; (2) an administrator password on a Windows box that does not expire; and (3) passwords not expiring for "super users" who have elevated privileges. Without accurate accounting, tracking, and reviewing of privileged users accessing Departmental systems and its resources, as well as not reviewing privileged user activities, the Department has no assurance that privileged user activity did not result in the compromise of its systems and data.

Position Risk Designations Were Not Consistently Documented for Background Investigations

Position risk designations were not consistently documented for background investigations. We judgmentally sampled 12 users (1 privileged and 11 nonprivileged) and requested evidence that a risk designation was performed for each user. The Department was unable to provide documented evidence that a risk designation was prepared for all 12 users. By not consistently documenting position risk descriptions, the Department has no assurance that the most qualified individuals are matched with proper positions.

Network Access Control Solution Allowed Reconnection After Blocking Unauthorized Device

Although the Department has progressed in further enabling functionality of its Network Access Control solution, we found that it is still not fully implemented. Prior audit findings dating back to FY 2011 found that the Department had not enabled its Network Access Control solution to restrict the use of personal devices or non-Government Furnished Equipment on its network. During our FY 2018 testing, we found that the Network Access Control would not allow our non-Government Furnished Equipment device to connect to the network. However, when we attempted to reconnect the device, we were allowed to connect in 90 second increments. Although OCIO believed unauthorized devices were being filtered and not allowed to connect to the Department's network, OCIO was made aware of this reconnection anomaly and is currently working to resolve the configuration deficiency. Any type of access to the network, even for a short period of time, can allow a malicious actor to launch an attack or gain intermittent access to internal network resources that could lead to data leakage or data exposure.

Two-Factor Authentication Was Not Fully Implemented

We found that FSA did not consistently enforce the use of two-factor authentication. For 653 FSA websites identified, we used the URL Profiler tool to assess the security posture and ensure that the websites were compliant with Federal guidance. Our testing disclosed that of the 653 websites, 21 were not configured to use two-factor authentication. Failure to implement two-factor authentication will allow a user with a username and password to remotely connect and access network resources. This unrestricted access could lead to leakage and data exposure. We reported a similar condition in our FY 2011 through FY 2017 FISMA audits.

Access Agreements Required Before Granting Access Were Not Consistently Documented

The Department did not consistently document access agreements for individuals before granting access to its systems. These agreements included non-disclosure agreements for privileged users with access to sensitive information, and Rules of Behavior. We judgmentally selected a sample of 12 users (1 privileged user and 11 nonprivileged users) and requested a signed Rules of Behavior acknowledgement and, if applicable, a non-disclosure agreement. For the one privileged user, we found that the Department had not documented a signed non-disclosure agreement. This particular user had administrative access to all computers in the Windows environment. Although the Department believed that non-disclosure agreements were not applicable, the Information Assurance Cybersecurity Policy states that "the Department requires that access to controlled assets, data, and information…be granted only after users have read, understood, and signed a non-disclosure agreement." In addition, the Department was not able to provide a signed Rules of Behavior acknowledgement for any of the 12 users. The Department stated that a user Rule of Behavior is used in conjunction with security training; however, the Department could not provide documentation that the 12 users acknowledged and signed a Rules of Behavior as part of their access agreements. Without applicable access agreements acknowledged and signed by users granted access to Departmental systems and resources, there is an increased risk that users may unintentionally disclose sensitive information or act in a manner contrary to Department policies, procedures and guidelines.

Terminated User Access Was Not Removed from the Department's Network

The Department did not remove user access for people who were terminated from employment. We received a list of 235 users whose employment was terminated from October 1, 2017, through April 23, 2018. Of those 235 users, we found 75 accounts where access had not been removed for more than 60 days. We also noted that of those 75 accounts, 1 user remained active on the network even though they were terminated during their probationary period, and 6 users had active Microsoft Outlook accounts. The Department stat that during our audit fieldwork, there was a lapse in the notification process for removing accounts from its network for a period of time. Terminated employees whose user accounts remained active with access to critical Department or FSA systems and resources increase the risk of unauthorized access by malicious users and compromise Departmental information resources.

Websites Were Not Configured to Display Warning Banners

We found that certain FSA websites were either missing warning banners, or banners were not displaying standard Federal regulation language. For 653 FSA websites, we used the URL Profiler tool to assess the security posture to ensure that websites complied with Federal guidance. We found that of the 653 websites, 66 were missing warning banners, or the banner was not displaying approved warning banner language. Department policies and NIST guidance mandate that users are provided a warning banner alerting them that they are accessing a Government website. At minimum, warning banners should state that users should not expect any privacy when connecting to an information technology asset owned or operated on behalf of the Department. The Department has communicated through the weekly ED Notebook update to stakeholders that banners with acceptable text are required to be in place by October 1, 2018. We reported a similar condition in our FY 2017 FISMA audit.

FSA's Controls Over Database Management Needed Improvement

We performed assessments that identified vulnerabilities, configuration errors, and access issues for databases included in three of our eight judgmentally selected system sample—the Next Generation Data Center General Support System (consisting of five databases), the Person Authentication Service; and the Student Aid Internet Gateway.

Our scans of databases associated with these systems identified a total of 96 high vulnerabilities, 123 medium vulnerabilities, and 54 low vulnerabilities. We shared the vulnerabilities with OCIO and FSA for remediation. By allowing these vulnerabilities to exist, the Department increases the risk that unauthorized individuals can access or alter the data. We reported similar conditions in our FY 2017 audit.

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.

The lack of internal controls and safeguards governing the identity and access management could increase the risk of system compromise.

<u>Virtual Private Network Connections Were Not Disconnected After 30 Minutes of Inactivity</u>

During our testing of FSA's databases, we found that the virtual private network connection did not disconnect the user after 30 minutes of inactivity. During the testing process, we connected to the virtual private network and were authenticated by using a username, password, and token. Once connected, we validated that after 30 minutes of inactivity, the user was not disconnected from the network. In two separate testing occasions, the connection remained online for over 3 days without being disconnected from the network. In addition, we requested logs from FSA to validate the virtual private network connections, duration time, and time of disconnect. However, FSA did not provide the logs during our fieldwork. Without a properly functioning virtual private network time-out feature, users could increase the risk that the Department's networks are exposed to unauthorized users and compromise the confidentiality, integrity, and availability of information systems. We reported a similar condition in our FY 2011, FY 2012, and FY 2015 FISMA audit reports.

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. (Repeat Recommendation)

3.2 Ensure that position risk designations are documented for background investigations.

3.3 Enforce a two-factor authentication configuration for all user connections to systems and applications. (Repeat Recommendation)

We recommend that the Deputy Secretary require to OCIO—

3.4 Finalize Departmental Directive OM: 5-101, "Personnel Security Screening Requirements for Contractor Employees."

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

3.6 Ensure the Network Access Control solution is configured to disallow users to reconnect devices after being blocked.

3.7 Ensure access agreements—in particular non-disclosure agreements for privileged users with access to sensitive information, and Rules of Behavior acknowledgements—are documented for users accessing Department and FSA systems.

3.8 Ensure that terminated individual's network access is removed timely.

We recommend that the Chief Operating Officer require FSA to—

3.9 Establish a process for identifying, managing, and tracking activity of privileged user accounts. (Repeat Recommendation)

3.10 Configure all websites to display warning banners when users login to Departmental resources and ensure that banners include approved warning language. (Repeat Recommendation)

3.11 Create corrective action plans to remedy database vulnerabilities for all database vulnerabilities identified. (Repeat Recommendation)

3.12 Validate the inactivity settings to ensure sessions are timing out after 30 minutes of inactivity. (Repeat Recommendation)

Management Comments

The Department concurred with recommendation 3.1, 3.2, 3.4, 3.5, 3.7, 3.8, 3.9, 3.10, 3.11, and 3.12; partially concurred with recommendation 3.3; and did not concur with recommendation 3.6. For recommendations 3.1, 3.2, 3.4, 3.5, 3.7, 3.8, 3.9, 3.10, 3.11, and 3.12, the Department stated it will develop corrective action plans by December 31, 2018 to address the associated finding.

For recommendation 3.3, the Department stated that it has completed a number of activities to address this issue. This included an analysis of the Department Information Technology systems that was conducted in fiscal year 2018 to align with the new Digital Identity Guidelines outline in the revised version of NIST SP 800-63-3, revision 3 and supplemental guidelines (NIST SP 800-63A, NIST SP 800-63B, and NIST SP 800-63C). The analysis resulted in a revised "ED Systems and Applications Assurance Levels Baseline" covering the new terminology of identity, authentication and federation assurance levels. For systems that were determined to require enhanced authentication requirements, Plan of Actions and Milestones were developed and tracked in the Department's system inventory.

For recommendation 3.6, the Department did not concur and stated it has implemented additional mitigations to reduce the potential risk of unauthorized devices while also reducing the time needed to block an authorized device.

OIG Response

OIG will review corrective action plans to determine if the actions will address the finding and recommendations and if so, will validate during our FY 2019 FISMA audit fieldwork.

OIG will validate the corrective actions for recommendation 3.3 to determine if they will address the finding and recommendation during our FY 2019 FISMA audit fieldwork.

Although the Department explained that it implemented mitigations to reduce the potential risk of unauthorized devices and did not concur with recommendation 3.6, it has not identified specifically what mitigations it implemented. Without specific identification of what mitigations the Department implemented, the OIG cannot assess the mitigations to determine if they actually address the weakness we identified. Also, until immediate blocking of unauthorized devices is achieved, a skilled malicious actor still has the ability to launch an attack or gain intermittent access to internal network resources.

METRIC DOMAIN 4—DATA PROTECTION AND PRIVACY

Personally identifiable information is any information about an individual maintained by an agency including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Treatment of personally identifiable information is distinct from other types of data because it needs to be not only protected, but also collected, maintained and disseminated in accordance with Federal law. Protecting the privacy of individuals' personally identifiable information is collected, used, maintained, shared, and disposed of by programs and information systems, is a Fundamental responsibility of federal organizations.

We determined that the Department's and FSA's data protection and privacy programs were consistent with the Defined level of the maturity model. The Data Protection and Privacy metric domain is a new area that was created as part of the FY 2018 IG FISMA Metrics. Therefore, this was the first year we assessed this area for its level of effectiveness.

The Department's Office of the Privacy Officer was established in 2010 and includes involvement by the chief privacy officer, the Privacy Safeguards Division, the

Department's Incident Response team, and the Education Security Operations Center. The Department has also established a Privacy Incident Response Team and Privacy Advisory Group that include Department officials such as the senior official in each affected principal office, chief information officer, chief information security officer, general counsel, Assistant Secretary for Communications and Outreach, Assistant Secretary for Legislation and Congressional Affairs, and Assistant Secretary for Management.

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

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

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

As part of the Department's data protection and privacy process, it established the use of Privacy Impact Assessments, System of Records Notice, and Privacy Threshold Analyses. A Privacy Impact Assessment is an analysis of how information in identifiable form is collected, maintained, stored, and disseminated. The assessment also examines and evaluates the privacy risks and the protections and processes for handling information to mitigate those privacy risks. Privacy Impact Assessments are reviewed every two years to determine whether any significant changes have occurred that create new privacy risks. A System of Records Notice informs the public about what kinds of protected personal information Federal agencies maintain, limits the uses and disclosures of the information to those compatible with the law permitting its collection, and describes how an individual might request access to their information or to seek redress otherwise. A Privacy Threshold Analysis is a short form used to determine whether a system contains personally identifiable information, whether a Privacy

Impact Assessment or System of Records Notice is required, and whether any other privacy requirements apply to the information system.

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

The Department's Breach Response Plan included the requirement for the Privacy Incident Response Team to perform annual tabletop exercises. However, the Department had not conducted a tabletop exercise, as discussed in the finding section below.

The Privacy Office stated that it does not have the resources to administer a privacy training program across the Department; therefore, they coordinate with OCIO to develop training that includes privacy topics that are then included in annual security awareness training requirements.

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

We found that for the Data Protection and Privacy metric domain, the Department and FSA were Defined level for all five metric questions. The Department and FSA can strengthen their controls regarding data protection and privacy to enable them to progress to the next maturity level in the areas of (1) ensuring that the Handbook for Protecting Sensitive but Unclassified Information is current, (2) annually testing its Breach Response Plan, and (3) consistently and timely reviewing of Privacy Impact Assessments. In addition, we identified other areas impacting data protection and privacy that are addressed under other metric domains in this report.

Handbook For Protecting Unclassified Information Was Not Current

The Department established the Handbook for Protection of Sensitive But Unclassified Information. This directive provides all personnel, including employees and support contractors, with information necessary to protect sensitive but unclassified information from misuse, loss, or unauthorized disclosure. However, the Department had not updated this policy since 2007. Without updated guidance, the Department cannot ensure that privacy information is protected from misuse, loss, or unauthorized disclosure.

Breach Response Plan Was Not Annually Tested

We found that at the Department's Breach Response Plan had not been tested. The Department's Breach Response Plan requires the Privacy Incident Response Team to perform annual tabletop exercises to test the plan and ensure members of the team are familiar with the plan and understand their specific roles. The last tabletop exercise was conducted on May 11, 2017. As of May 22, 2018, the Department had yet to perform its annual exercise. Without testing the Breach Response Plan, the Department has no assurance that roles are properly executed in the occurrence of a breach.

Timely Review of Privacy Impact Assessments Were Not Consistently Performed

We found that the Department was not timely reviewing system Privacy Impact Assessments. The Department's Privacy Program Plan requires that Privacy Impact Assessments be reviewed every two years; however, from our review of our eight judgmentally selected systems, we found that the Department did not timely review the Privacy Impact Assessments for five systems. Specifically, two of the five systems had not been reviewed since 2008. By not consistently performing reviews of Privacy Impact Assessments every two years, the Department cannot ensure that systems reflect most current privacy risks.

Other Report Findings Impacting Data Protection and Privacy

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

OMB Circular A-130, "Managing Information as a Strategic Resource," July 28, 2016, requires Federal agencies to develop and maintain a privacy program plan that provides an overview of the agency's privacy program. This includes a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the senior agency official for privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks, and any other information determined necessary by the agency's privacy program. Also, the Departmental Directive "Personally Identifiable Information Breach Response Policy and Plan," states the senior agency official for privacy will, at least annually, convene the Privacy Incident Response Team to hold a tabletop exercise. In addition, the Department's Privacy Program Plan states that Privacy Impact Assessments are reviewed bi-annually to determine whether any significant changes have occurred that create new privacy risks.

Recommendations

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

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

We recommend that the Deputy Secretary require OCIO to—

4.2 Ensure that the Handbook for Protection of Sensitive But Unclassified Information is updated.

4.3 Ensure the Department's Breach Response Plan is tested annually.

4.4 Ensure that Privacy Impact Assessments are reviewed every two years.

Management Comments

The Department concurred with the recommendations and stated it will develop corrective action plans by December 31, 2018 to address the associated finding.

OIG Response

OIG will review the corrective action plans to determine if the actions will address the finding and recommendations and if so, will validate during our FY 2019 FISMA audit fieldwork.

METRIC DOMAIN 5—SECURITY TRAINING

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

We determined that the Department's security training program was consistent with the Defined level of the maturity model. The Department established the Cybersecurity Workforce Development Strategy and Program Plan showing how it plans to identify, expand, recruit, retain, and sustain a capable and competent workforce in key functional areas to address evolving cyber threats. The Department also created the Learning and Developmental Division that is responsible for developing training in accordance with NIST SP 800-181, “National Cybersecurity Workforce Framework.” Furthermore, the Department established a phishing program that includes a three simulated phishing exercises each fiscal year and uses the results to help determine what areas to focus on for future exercises.

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 an effective level of maturity, the Department would need to achieve that level in at least four of the six metric questions. For example, the Department would need to demonstrate that it has addressed deficiencies in developing staff knowledge, skills, and abilities. It would also have to demonstrate that skilled personnel have been hired and/or existing staff are continuously trained to have the appropriate skills and knowledge to protect the Department’s assets and information. Finally, the Department would need to develop and implement the appropriate metrics to measure the effectiveness of the organization’s training program in closing identified skill gaps.

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

The Department established the Cybersecurity Workforce Development Strategy and Program Plan that identifies how it plans to identify, expand, recruit, retain, and sustain a capable and competent workforce in key functional areas to address evolving cyber threats. It also incorporates that National Initiative for Cybersecurity Education Cybersecurity Workforce Framework that describes the knowledge, skills, and abilities needed to complete tasks that can strengthen the cybersecurity posture of an organization.

The Department also created the Learning and Developmental Division that is responsible for using NIST SP 800-181, “National Cybersecurity Workforce Framework,” to identify discrete specialty areas within the Department’s cybersecurity workforce for each role and identify cybersecurity workforce resources and skill gaps. In addition, the

Department is working with the Excellence in Government group, which will conduct pilot testing skill assessments on a sample of users and their roles. The Department also established a Cybersecurity Workforce Development/Training Program Working Group that helps identify, expand, recruit, retain, and sustain a capable and competent workforce in key functional areas to address complex and ever-evolving cyber threats.

The Department established a Cybersecurity Awareness and Training Program to help reduce risk to its systems and information assets by changing human behavior and inform its personnel about security risks associated with their activities and responsibilities. The Department's "Information Technology Cybersecurity Awareness and Training Program Tactical Plan for Fiscal Years 2017-2018" establishes a security training program that focuses on informing personnel of their responsibilities in complying with Departmental policies and procedures designed to reduce risks and support the continuous growth and development of the cybersecurity workforce.

The Department uses the annual Cybersecurity and Privacy Awareness training, covering employees and contractors, as one method of assessing whether staff has the knowledge, skills, and abilities to perform their assigned work. It offers three Cybersecurity and Privacy Awareness trainings each year to assess the skills and knowledge of employees and contractors. New employees and contractors are also required to participate in the Cybersecurity and Privacy Awareness training program prior to accessing the Department's network. The Department tracks employees and contractors who fail to take the Cybersecurity and Privacy Awareness trainings. In addition, the Department defined the process to assess personnel with significant security responsibilities to ensure that they receive appropriate training and education to develop and maintain a cyber security workforce capable of actively reducing and managing risk to its assets. During 2018, the administration and tracking of the Department's online security training was transitioned from the Talent Management System to Fed Talent.

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

In March 2018, the OCIO issued a memorandum, "Requirements for Role-Based Training of Personnel with Significant Security Responsibilities," that requires the Department to identify personnel with significant security responsibilities and provide security training commensurate with their responsibilities. The Department also developed the

Cybersecurity Awareness and Training Program Guidance, which establishes the requirements needed for system users to receive specialized training based on their roles and responsibilities. It also established a process to identify all positions within the agency that require the performance of information technology cybersecurity and assigned the corresponding Office of Personnel Management Cybersecurity Data Standard Codes to each of these positions after conducting an assessment of the knowledge, skills, and abilities of its cybersecurity personnel to determine the appropriate content of security training.

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

We found that for the Security Training metric domain, the Department and FSA to be at the Defined level for all six metric questions. The Department and FSA can strengthen their controls regarding security training to enable them to progress to the next maturity level in the areas of (1) implementing a formal skill assessment process; (2) implementing a process for identifying individuals requiring role-based training; (3) verifying new employee training completion before granting network access; and (4) suspending user accounts when required training is not completed immediately after the due date.

Department Had Not Fully Implemented a Formal Skill Assessment Process

The Department had not fully implemented a formal skills assessment process that assesses employees' educational level and experience in performing their job functions. Although initial knowledge, skills, and assessments were completed at an agency level, we found that the Department had not finished defining a formal process. For instance, the Department was still developing key assessments enabling supervisors to assess the workforce skills of their employees. The Department was working on how to implement NIST SP 800-181, "National Initiative for Cybersecurity Education Cybersecurity Workforce Framework," for assessing knowledge and skills of staff.

The Office of Personnel Management issued "Guidance for Identifying, Addressing, and Reporting Cybersecurity Work Roles of Critical Need" in April 2018. It states that by April 2019, agencies need to report their greatest skill shortages; analyze the root cause of the shortages; and provide action plans, targets and measures for mitigating the critical skill shortages. By not implementing a formal skill assessment process, users may not be acquiring the necessary skills that will enable them to perform their job function. We reported a similar condition in our FY 2016 FISMA audit.

Process for Identifying Individuals Requiring Role-Based Training Was Not Fully Implemented

We found that the Department had not fully implemented a process for identifying and providing role-based training. In March 2018, the Chief Information Security Officer issued a memorandum, "Requirements for Role-Based Training of Personnel with Significant Security Responsibilities" that describes the requirements for employees with significant security responsibilities to take role-based training. However, the Department was still in the process of identifying personnel with significant security responsibilities. According the Department, once all individuals are identified, they will receive role-based training. Without identifying and providing role-based training, a user may not possess the adequate knowledge and skills necessary to assist them in carrying out their job function in a secure manner.

New User Training Completion Could Not Be Verified Before Access

We found that the Department could not verify that all new users completed required security training before they accessed the Department's network. We received a list of 304 new users (57 Federal and 247 contractor employees) that started employment with the Department from October 2017 through January 2018. For 12 contractor employees we judgmentally selected, we found that 8 accounts were established before the employee completed security training. For these accounts, the Department could not identify the date the user first accessed the system and, therefore, we could not determine whether the user accessed the system before completing the required training. Currently, it is the responsibility of the system owners and contracting officer representatives to ensure that contractor employees complete the training for access, suspension, and termination of contractor employee user accounts. If employees do not fulfill training requirements before accessing the network, the Department has no assurance that new users have appropriate knowledge to protect Department assets from compromise. We identified a similar condition in our FY 2017 FISMA audit.

Users Accounts Were Not Suspended Timely When Users Failed to Complete Required Training

We found that both Department and contractor employee network accounts were not timely suspended when users did not complete required training. In March 2018, we received a list of 610 employees (5 Federal and 605 contractor employees) who did not complete the required Cybersecurity and Privacy Awareness -1 training by the required deadline of March 2, 2018. We judgmentally selected a sample of 18 users (all 5 Federal and 13 contractor employees) to determine whether their accounts were suspended after the training completion deadline. We found that all accounts were suspended on March 12, 2018, ten days after the completion deadline. In June 2018, we also received a list of 228 employees (5 Federal and 223 contractor employees) who did not complete the required Cybersecurity and Privacy Awareness -2 training by the required deadline of May 25, 2018. We judgmentally selected a sample of 19 users (all 5 Federal and 14 contractor employees) to determine if their accounts were suspended after the completion deadline. For all 19, the Department could not identify a suspension date; therefore, we could not determine whether the accounts were suspended timely. During our discussions with the Department, we verified that account suspension is currently a manual process, rather than an automated one. By not suspending user accounts for individuals who have not completed required security training, the Department cannot ensure information resources are accessed by properly trained users.

OMB Circular A-130, "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 Chief Information Officers to ensure that effective tracking and reporting mechanisms for security training are in place.

Recommendations

We recommend that the Deputy Secretary require OCIO to—

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

5.2 Ensure that contractor employees fulfill mandatory training requirements before accessing Department systems. (Repeat Recommendation)

5.3 Define and implement a process to track contractors' initial access to the Department's network.

5.4 Ensure that user accounts are suspended timely when users do not complete required training.

5.5 Implement the process for identifying employees with significant security responsibilities and ensure role-based training is provided.

5.6 Implement the process for formal skill assessments of employees' educational level and experience to begin full reporting to the Office of Personnel Management by April 2019.

Management Comments

The Department concurred with recommendations 5.1, 5.2, 5.3, 5.5 and 5.6, and partially concurred with recommendation 5.4. For recommendations 5.1, 5.2, 5.3, 5.5 and 5.6, the Department will develop corrective action plans by December 31, 2018 to address the associated finding.

For recommendation 5.4, the Department stated that while they recognize that efficiencies in its processes can be improved, it believes it unreasonable and a possible negative impact to business operations to immediately suspend user accounts in an automated fashion for failure to compete cybersecurity awareness training by the established due date. However, it proposed a corrective action plan by December 31, 2018 to address the recommendation.

OIG Response

OIG will review the corrective action plans to determine if the actions will address the finding and recommendations and if so, will validated during our FY 2019 FISMA audit fieldwork.

OIG will review the corrective action plan to determine if the actions will address the finding and recommendation and if so, will be validated during our FY 2019 FISMA audit fieldwork.

Regarding the Department's response to recommendation 5.4, its "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. Therefore, to be consistent with its guidance, the Department will need to ensure that users complete the required training to continue their network access and suspend those accounts who fail to meet this requirement. OIG will review the corrective action plan to determine if the actions will address the finding and recommendation and if so, will validated during our FY 2019 FISMA audit fieldwork.

SECURITY FUNCTION 3—DETECT

The "Detect" security function comprises the ISCM metric domain. Based on our evaluation of the Department's ISCM program, we determined the Detect security function was consistent with the Defined level of the maturity model, which is categorized as being not effective. We found that the Department and FSA established policies and procedures consistent with NIST guidelines and OMB policy; and communicated ISCM issues through Risk Management Framework Workshops, quarterly Cybersecurity Forums, and monthly Cybersecurity Framework Risk Scorecards. 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 (1) fully implementing the Department's ISCM strategy; (2) ensuring that all ISCM stakeholders establish and use accounts within the Cyber Security Assessment and Management tool; and (3) fully implementing the Continuous Diagnostics and Migration program.

METRIC DOMAIN 6—INFORMATION SECURITY CONTINUOUS MONITORING

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

We determined that the Department's and FSA's ISCM programs were consistent with the Defined level of the maturity model. The Department used the ISCM Enterprise Roadmap as its enterprise-wide ISCM strategy. In addition, it also participated in the DHS Continuous Diagnostics and Mitigation program. The Department and FSA established their own security assessment process for their respective systems (Continuous Security Assessment process and Ongoing Security Authorization process). However, while the Department has made several improvements to its ISCM program, its practices in several areas still did not meet the Managed and Measurable threshold under the metrics to be considered effective. To meet an effective level of maturity, the Department would need to achieve that level for 3 of the 5 metric questions. For example, the Department would need to demonstrate that its staff was consistently collecting, monitoring, and analyzing qualitative and quantitative performance measures across the organization and reporting data on the effectiveness of the organization's ISCM program.

The Department developed policies, procedures, and guidance to assist in implementing and supporting its ISCM Enterprise Roadmap and overall implementation of its ISCM program. The Department used the ISCM Enterprise Roadmap as its enterprise-wide ISCM strategy, which was updated in April 2017. Components within the Department worked together daily to ensure that risk management was integrated into its ISCM Enterprise Roadmap and overall ISCM program and was communicated through Risk Management Framework Workshops, quarterly Cybersecurity Forums, and monthly Cybersecurity Framework Risk Scorecards. In addition, the Department developed its Cybersecurity Risk Management Framework that was incorporated in its enterprise-wide Risk Management strategy.

The Department was participating in DHS's Continuous Diagnostics and Mitigation program. The Department had partially implemented its DHS Continuous Diagnostics and Mitigation capabilities for Phase 1: Hardware Asset Management, Software Asset Management, Configuration Settings Management, and Vulnerability Management. The Department was able to fully integrate its Agency Continuous Diagnostics and Mitigation Dashboard with the Federal Continuous Diagnostics and Mitigation Dashboard. The Department provided multiple rounds of training on the dashboard to its employees last year.

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

Both the Department and FSA established their own security assessment process for their respective systems. We obtained the system schedule for both processes and determined that all eight judgmentally selected systems for this year's review were included in both the Department's and FSA's processes and had current Authorizations to Operate.

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

Finding 6. The Department's ISCM Program Needs Improvement (Repeat Finding)

We found that for the ISCM metric domain, the Department and FSA were at the Defined level for four metric questions, and at the Managed and Measurable level for one metric question. The Department can strengthen its controls regarding ISCM, which will enable it to progress to the next maturity level in the areas of (1) fully implementing ISCM strategy and policies, (2) fully implementing its Continuous Diagnostics and Mitigation program, and (3) ensuring ISCM Stakeholders are able to perform monitoring functions in the Cyber Security Assessment and Management tool.

ISCM Strategy and Policies Were Not Fully Implemented

Although the Department developed and communicated its ISCM Roadmap (enterprise strategy) inclusive of all required components and used a monthly Cybersecurity

Framework Risk Scorecard to monitor and communicate high level risks, it had not consistently or effectively implemented its strategy regarding the collection and monitoring of all defined metrics for its operational systems. Specifically, based on a judgmental sample of eight systems, we determined that the Department did not maintain monthly hardware inventory reports and monthly software inventory reports in the Cyber Security Assessment and Management tool for seven systems. In addition, we determined that the Department did not maintain monthly vulnerability scan result reports and monthly configuration setting scan result reports in the Cyber Security Assessment and Management tool for the eight systems. We also determined that the Department did not develop system-specific continuous monitoring plans for any of the eight sampled systems. By implementing an automated security control process, the Department can help ensure that it maintains an effective ISCM program for its security controls. We reported a similar condition in our FY 2017 FISMA audit.

DHS Continuous Diagnostics and Mitigation Program Was Not Fully Implemented

Although the Department has made progress in the implementation of DHS Continuous Diagnostics and Mitigation phase components, such as the completion of the Continuous Diagnostics and Mitigation Federal Dashboard integration, it has not completed the implementation of Phase 1 or Phase 2 of the program. In addition, the Department completed the alignment of its Department policies with that of the DHS Continuous Diagnostics and Mitigation program; however, it had not consistently implemented the collection of metrics across all of its operational systems. By not fully implementing a CDM program, the Department cannot ensure that security controls are adequately monitored to help protect its information technology assets and information. We reported a similar condition in our FY 2017 FISMA audit.

ISCM Stakeholders Were Unable to Perform Monitoring Functions in the Cyber Security Assessment and Management Tool

Although the Department defined and communicated the structures of its ISCM team and the roles and responsibilities of ISCM stakeholders, these roles and responsibilities were not consistently implemented to effectively implement ISCM activities. Specifically, the Department identified 115 operational systems across the organization with required points of contact who did not have an account in the Cyber Security Assessment and Management tool. Specifically, across these 115 operational systems, a total of 50 individuals (24 authorizing officials and 26 information system owners – one of whom was also an information system security officer) that did not have an account in the Cyber Security Assessment and Management tool as of July 1, 2018. We reported a similar condition in our FY 2017 FISMA audit.

These conditions occurred because the current process for collecting and monitoring defined ISCM metrics is manual. In addition, the Department stated that the eight sampled systems were not yet included in the DHS Continuous Diagnostics and Mitigation pilot. Further, no established Department policy requires ISCM stakeholders (i.e., authorizing officials, information system security officers) to establish accounts within the Cyber Security Assessment and Management tool. Without access to the Cyber Security Assessment and Management tool, stakeholders cannot ensure that they have the ability to monitor ongoing security concerns impacting their respective systems.

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

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

Recommendations

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

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

We recommend that the Deputy Secretary require OCIO to—

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

6.3 Ensure that ISCM stakeholders with designated roles and responsibilities are properly educated and engaged. (Repeat Recommendation)

6.4 Ensure all information authorizing officials, information system owners, and information system security officers establish and use accounts within the Cyber Security Assessment and Management tool, and that required points of contacts are identified. (Repeat Recommendation)

6.5 Ensure the completion of Phases 1 and 2 of the Continuous Diagnostics and Mitigation program. (Repeat Recommendation)

Management Comments

The Department concurred with the recommendations and stated it will develop corrective action plans by December 31, 2018 to address the associated finding.

OIG Response

OIG will review the corrective action plans to determine if the actions will address the finding and recommendations and if so, will validate during our FY 2019 FISMA audit fieldwork.

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 and FSA established policies and procedures consistent with NIST guidelines and OMB policy; established an incident response process, participated in the DHS EINSTEIN program[16]; deployed numerous incident response tools; and established a process for enterprise level incident reporting requirements. However, we noted some improvements were needed to help the agency reach a higher level of maturity. For instance, we found (1) categorizing and reporting incidents to the United States Computer Emergency Readiness Team (US-CERT) and OIG needed improvement, and (2) data loss prevention tools were not working as intended.

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

METRIC DOMAIN 7—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 information technology services. The goal of the incident response program is to (1) provide surveillance, situational monitoring, and cyber defense services; (2) rapidly detect and identify malicious activity and promptly subvert that activity; and (3) collect data and maintain metrics that demonstrate the impact of the Department's cyber defense approach, its cyber state, and cyber security posture.

We determined that the Department's incident response program was consistent with the Defined level of the maturity model. The Department established roles and responsibilities for incident management. In addition, it implemented various technologies to manage its incident response process. Further, it established a high-level strategy for containment, eradication, and recovery of incidents. Although the Department made several improvements to its incident response program, its practices in several areas still did not meet the Managed and Measurable threshold under the metrics to be considered effective. To achieve an effective level of security, the Department would need to achieve that level for at least four of the seven metric questions. For example, the Department would need to demonstrate that it had the ability to manage and measure the impact of successful incidents, used incident response metrics to measure and manage the timely reporting of incident information to its officials and external parties, and ensured data supporting the incident response metrics were accurate, consistent, and in a reproducible format.

The Department established policies, procedures, and guidance to define its incident response process. The Department also established roles and responsibilities for incident management. Both the Department and FSA established their own Security Operations Centers that provide integrated capabilities that use the Distributed Incident Response Team Model. The Department's Security Operations Center provides coverage 24 hours per day, 7 days a week. The Cyber Security Operations Education Security Operations Center Roles and Responsibilities further details the responsibilities of individual Education Security Operations Center team members relating to incident handling. In addition, the directive "Personally Identifiable Information Breach Response Policy and Plan" defines roles and responsibilities for incidents that involve breaches of personally identifiable information.

The Department implemented various technologies to manage its incident response process. For instance, it employs web application protection, event and incident management, aggregation and analysis, malware detection, and information management.

In 2009, the Department entered into an Interagency Shared Agreement with DHS to participate in the EINSTEN program. This enabled the Department to use EINSTEIN for intrusion detection capabilities for traffic entering and leaving its network. The Department fully deployed EINSTEIN 1 and 2 capabilities through a trusted internet connection. Further, the Department fully deployed EINSTEIN 3 Accelerated and was using it to detect and prevent potential compromises. The Department also had an Enhance Shared Situational Awareness Multilateral Information Sharing Agreement that enabled it to enhance its cybersecurity information sharing among Federal agencies.

The Department established a process detailing with attack vectors taxonomy that conform to the reporting requirements for US-CERT, the Department's incident categorizations, and incident prioritization. Specifically, the Department developed playbooks that included US-CERT reporting procedures and job aids to further list the threat vectors and incident categories in a template format. The Department also detailed a high-level strategy for detecting and analyzing incidents. The Department's playbooks also included various procedures, job aids, and check lists for handling different types of incidents.

The Department established a high-level strategy for containment, eradication, and recovery of incidents. The Department also used multiple check lists for containment strategy. Based on our review of incident logs from October 1, 2017 through July 27, 2018, we found that the Department has consistently implemented its containment strategies, eradication processes, and process to remediate vulnerabilities that could have been exploited.

The Department established a process for enterprise level incident reporting requirements. For instance, it established a detailed coordination process between both the Department and FSA Security Operations Centers of when and how system users should report events. For reporting security incidents to US-CERT and the OIG, the Department developed reporting procedures.

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

We found that for the Incident Response metric domain, the Department was at the Managed and Measurable level for one metric, the Consistently Implemented level for one metric, and the Defined level for five metrics. The Department can strengthen its controls regarding incident response to enable it to progress to the next maturity level in the areas of (1) categorizing and reporting incidents consistently to US-CERT and OIG, and (2) ensuring data loss prevention tools work accordingly.

Incidents Were Not Consistently Categorized and/or Reported to US-CERT and OIG

The Department used a prioritization scale that identified different types of incidents as categories. The categories range from 0 to 6, with category 1 having the highest criticality. The Department's policy required incidents in categories 1 through 4 be reported to US-CERT and the OIG. However, we found that incidents were not consistently categorized and reported to US-CERT and the OIG, as applicable. We reviewed 2,753 incidents created from October 1, 2017, through July 27, 2018. Of those, we found that 94 incidents were not consistently categorized according to the categories defined by Department policy, procedures, and guidance. For instance, we found some phishing campaign events were assigned a category 3, but they should have been assigned a Category 5. We also found that of the 76 category 4 incidents, 46 were not reported to US-CERT and 39 were not reported to the OIG.[17] Failure to report these incidents impedes the OIG's investigative responsibilities to secure vital evidence, make important connections to ongoing cases, or make decisions about initiating new cases. We reported a similar condition in our FY 2017 FISMA audit.

Table 4. Number of Incidents the Department Identified by Categorization Level

Category	Description	Number Identified
CAT 6	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	622
CAT 5	Any activity that seeks to access or identify a Federal agency computer, open ports, protocols, service, or any combination for later exploit.	1,799
CAT 4	A user violating acceptable computing use policies.	76
CAT 3	Successful installation of malicious software that infects an operating system or applications.	211
CAT 2	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources.	2
CAT 1	Individual gains logical or physical access without permission to a Federal agency network, system, application, or data.	36
CAT 0	Exercises and approved testing activity.	7

[17] A category 4 incident is considered a reportable incident to US-CERT and/or OIG.

In addition, of the 622 category 6 incidents, which did not require reporting, 28 were reported to US-CERT and 303 were reported to OIG. [18] The incidents were reported because they were initially classified as Category 6. However, the initial categorization level was not updated in the Department's incident tracking records to reflect the categorization level that was reported to US-CERT and OIG. According to Education Security Operations Center staff, incidents can be assigned with an initial category (e.g., category 6), but can be classified as a different category once more information becomes available and the Education Computer Incident Response Capability Coordinator decides which incidents to report. We reported a similar condition in our FY 2017 FISMA report.

The Department's Data Loss Prevention Tools Were Not Effective

Although the Department implemented various incident response tools and technologies (in the areas of web application protection, event and incident management, aggregation and analysis, malware detection, and information management), their deployment was divided by environments and did not cover all components of the Department's network. For example, the Education Security Operations Center and FSA's Security Operations Center separately to aggregate and analyze information from different sources and is not an enterprise-wide security information and event management aggregator. The Department recognized this challenge and stated that its ultimate goal is to have the tools and technologies implemented at the enterprise level when funding is available.

We also found that the Department's data loss prevention tools implemented for endpoint and Office365 were not effective. We performed tests by transmitting unencrypted numeric strings that mimicked Social Security number patterns through Microsoft Outlook on both the EDUCATE and Citrix desktop environments to internal and external recipients. According to the Department's announcement on its data loss prevention tools, if an email contains unencrypted social security numbers or numeric strings that appear to be social security numbers, the sender will receive a pop-up warning message and/or the email will be blocked. However, the Department's data loss prevention tools did not detect any of the transmissions in our testing; no pop-up messages appeared with the warning and no transmissions were blocked. In addition, we obtained and reviewed data loss prevention tool event logs and confirmed that no events were identified for the tests we performed. We reported a similar condition in our FY 2016 FISMA audit.

[18] A Category 6 incident is used to classify an incident under investigation due to insufficient data and considered "not an incident" and is not required to be reported to US-CERT and/or OIG.

OMB and NIST guidelines[19] 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 information technology systems.

Recommendations

We recommend that the Deputy Secretary require OCIO to—

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

7.2 Ensure that incidents are consistently submitted to US-CERT and the OIG within the required timeframe and all incidents are consistently categorized. (Repeat Recommendation)

7.3 Enable incident response tools and technologies to function on an enterprise basis.

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

Management Comments

The Department concurred with recommendation 7.1, and 7.3; partially concurred with recommendation 7.2; and did not concur with recommendation 7.4. For recommendations 7.1 and 7.3, the Department stated it will develop corrective action plans by December 31, 2018 to address the associated finding

For recommendation 7.2, the Department stated that it agreed that there are efficiencies that can be gained in incident management process. However, it pointed

[19] 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.

out that approximately two percent of all incidents were reported as incorrectly categorized. The Department said it reported tickets based on current reporting guidance listed in the Federal Incident Notification Guidance, and that tickets for similar alerts may be categorized as a Category 1, Category 2, or Category 3 depending on the severity of the event. It further stated that the differences in categorization for such alerts are not due to inconsistency, but rather because the events involved a different set of circumstances. As such, the Department believes it is unrealistic to achieve 100 percent accuracy at any point in time. The Department stated it will develop a corrective action plan by December 31, 2018 to address the recommendation.

For recommendation 7.4, the Department stated the configuration of the data loss prevention already works as intended.

OIG Response

OIG will review corrective action plans to determine if the actions will address the finding and recommendations and if so, will validate during our FY 2019 FISMA audit fieldwork.

For the Department's response to 7.2, we don't believe the two percent represents an accurate representation of the incidents, as this percentage included incidents that were not required to be reported, such as incidents in categories 5 and 6. For instance, the policy states that all incidents for category 1 through 4 must be reported to US-CERT. However, our analysis showed that 46 out of 76 reportable category 4 incidents, or 61 percent, were not reported to US-CERT. Further, we found that 39 out of 76 reportable category 4 incidents, or 51 percent, were not reported to the OIG.

OIG does not agree with the Department's assertion that the configuration of data loss prevention already works as intended. During our audit fieldwork, we tested the Department's data loss prevention solution by sending unencrypted emails containing fictitious personally identifiable information through the network. In a test conducted on July 25, 2018, OIG sent an unencrypted email containing personally identifiable information wording identifiers such as "date of birth" (with a numeric date), "social security number" (with a fictitious number), "bank account" (with a fictitious number), "check number" (with a fictitious number), "routing number" (with a fictitious number), and "account number" (with a fictitious number). In addition, the same email was sent again, unencrypted, on October 26, 2018. On both transmission dates, the sender did not receive a warning notification that possible personally identifiable information was being transmitted, or have the email blocked. Therefore, based on these tests, we do not believe the Department's data loss prevention solution is working as intended.

SECURITY FUNCTION 5—RECOVER

The “Recover” security function comprises the Contingency Planning metric domain. Based on our evaluation of the Department’s contingency planning program, we determined the Recover security function was at the Consistently Implemented level of the maturity model, which is categorized as being not effective. We found that the Department and FSA established policies and procedures consistent with NIST guidelines and OMB policy, defined and communicated roles and responsibilities across the organization, developed a comprehensive disaster recovery process, and maintained a centralized repository for storing and tracking contingency planning documentation. However, we noted some improvements were needed to help the agency reach a higher level of maturity. For instance, we found improvements were needed in enterprise skill assessment and accuracy and completeness of the contingency plan documentation.

METRIC DOMAIN 8—CONTINGENCY PLANNING

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

We determined that the Department’s and FSA’s Contingency Planning programs were consistent with the Consistently Implemented level of the maturity model. Roles and responsibilities for contingently planning were defined and communicated across the organization, including appropriate delegations of authority. System owners conducted annual contingency plan tests that included enterprise-wide exercises, as well as table-top exercises. Although the Department made several improvements to its Contingency Planning program, its practices in several areas still did not meet the Managed and Measurable threshold under the metrics to be considered effective. To achieve an effective level of security, the Department would need to achieve that level for at least four of the seven metric questions. For example, the Department would need to demonstrate that it employed automated mechanisms to more thoroughly and effectively test system contingency plans.

The Department and FSA defined its 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. In addition, the Department developed and maintained up-to-date Contingency Plan and Business Impact Analyses documents.

Roles and responsibilities for contingency planning were defined and communicated across the organization, including appropriate delegations of authority. Requirement(s) were also documented in contingency plans, the Department's Continuity of Operations Plan, Office of Management's Continuity of Governance Plan, and system specific contingency plans. Furthermore, roles and responsibilities are communicated across the organization, including appropriate delegations of authority, the Information Assurance Cybersecurity Policy, as well as contingency plan guidance. This guidance identifies the roles and responsibilities for specific use of the contingency planning and testing.

The Department established a Business Impact Analysis process that included identifying essential information technology resources, identifying disruption impacts and allowable outage times, and developing recovery priorities. The results of these analyses were incorporated in each system's contingency plan. The system owners and information system security officers were responsible for Business Impact Assessments, as well as creating and maintaining the impact assessment authorization processes to comply with FISMA. A Business Impact Assessment evaluation was performed annually and reviewed by OCIO risk management contractors during system accreditation. The Department's methodology used to develop the Business Impact Assessment complied with NIST guidance, as well as the Department's Contingency Planning Guide for Information Technology Systems.

The Department developed and maintained contingency plans for information systems that were updated at least annually and stored within the Cyber Security Assessment and Management tool. Contingency plans were used as part of the Department's risk management scoring, developing corrective action plans, as well as the Cybersecurity Framework Scorecard, and were reviewed by the system owners and independent assessors. The plans also addressed relevant recovery elements such as backup, alternate backup, and recovery priorities. Our review of eight judgmentally selected systems found that backup information was incorporated within each system's contingency plan.

The Department established alternate processing and storage facilities that were configured with information security safeguards equivalent to those of the primary site. Also, backups of information relating user and system were consistently performed and the confidentiality, integrity, and availability of this information are maintained. Further, the planning and performance of recovery activities were consistently communicated to relevant stakeholders and executive management teams, who use the information to make risk based decisions.

System owners were required to conduct annual contingency plan tests that included enterprise-wide exercises, and table-top exercises. In May 2018, we observed the annual EDUCATE disaster recovery test. By attending pre-disaster recovery exercise meetings, we verified that preparations took place, and we ensured that plans and objectives were outlined and documented. We also participated in a live status update meeting that occurred during the test to ensure that recovery efforts were executed in accordance with documented plans and monitored to ensure that systems were recovered successfully. We verified that any problems were recorded and tracked, resolution was achieved, and results were communicated to management. We found that the Department consistently captured and shared lessons learned on the effectiveness of information system contingency planning policies, procedures, strategy, and processes. The Department's planning and performance for the recovery activities were primarily communicated using the Cybersecurity Framework Scorecards, Secretary briefings, and Risk Management forums.

Finding 8. The Department's and FSA's Contingency Planning Program Needs Improvement (Repeat Finding)

We found that for the Contingency Planning metric domain, the Department and FSA were at the Defined level for two metric questions, the Consistently Implemented level for three metric questions, and Managed and Measurable level for two metric questions. The Department and FSA can strengthen their controls regarding contingency planning to enable them to progress to the next maturity level in the areas of (1) enterprise skill assessment; and (2) documenting contingency planning and testing results.

Enterprise Skill Assessment Was Not Performed

Although the roles and responsibilities of stakeholders involved in information system contingency planning were fully defined and communicated across the organization, Department workforce skills were not being measured at the enterprise level. We first identified this condition in the FY 2017 FISMA audit, and the Department committed to update its Cybersecurity Strategy Implementation Plan to ensure that skill assessments were performed at the enterprise level. It also committed to leveraging the Cybersecurity Strategy Implementation Plan document and available automated tools to assess the knowledge, skills, and abilities of the Department's workforce and tailor specialized training and identify skill gaps for all cybersecurity positions. However, neither of the two recommended actions had been completed during our fieldwork.

The Office of Personnel Management issued "Guidance for Identifying, Addressing, and Reporting Cybersecurity Work Roles of Critical Need" in April 2018. It stated that by April 2019, agencies need to report their greatest skill shortages; analyze the root cause of the shortages; and provide action plans, targets and measures for mitigating the critical skill shortages. By performing enterprise skill assessments, the Department can ensure that personnel have the required knowledge, skills and abilities to consistently carry out their job functions.

Contingency Plan and Testing Documentation Were Not Consistently Updated

Although the Department established and maintained an enterprise-wide business continuity/disaster recovery program, we found the Department was not consistent and timely documenting its contingency planning information. Specifically, out of the eight judgmentally selected systems we reviewed, four did not have current contingency plans. For three systems, we were unable to find evidence of annual testing of contingency plans. In addition, we identified other relevant planning documents that were not up to date with current requirements. Specifically, we identified four system security plans that were outdated, with one plan dating back to 2015. Although the Department uses the Cyber Security Assessment and Management tool to maintain a central repository for all its information system documentation, the tool has no automated capabilities for its contingency planning documentation. By not testing systems contingency plans, the Department has no assurance that it will be able to recover its resources in the event of a disaster. We reported similar conditions in our FY 2012, 2014, and 2015 FISMA audits.

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.[20] Without ensuring that skill assessments are performed at the enterprise level, necessary planning and testing documentation 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 information technology resources in the event of a disaster.

Recommendations

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

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

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

8.2 Ensure that contingency planning documentation and results of contingency plan testing are documented consistently and timely. (Repeat Recommendation)

We recommend that the Deputy Secretary require OCIO to—

8.3 Ensure that skills are being measured at the enterprise level to begin full reporting to the Office of Personnel Management by April 2019. (Repeat Recommendation)

Management Comments

The Department concurred with the recommendations and stated it will develop corrective action plans by December 31, 2018 to address the associated finding.

OIG Response

OIG will review the corrective action plans to determine if the actions will address the finding and recommendations and if so, will validate during our FY 2019 FISMA audit fieldwork.

Appendix A. Scope and Methodology

Our objective was to determine whether the Department's and FSA's overall information technology security programs and practices were effective as they relate to Federal information security requirements. For FY 2018, the IG reporting metrics were organized around the five information security functions outlined in NIST's Framework for Improving Critical Infrastructure Cybersecurity: Identify, Protect, Detect, Respond, and Recover. To meet the objective, we conducted audit work and additional testing in the eight metric domains associated with the security functions identified in the framework: (1) Risk Management (2) Configuration Management, (3) Identity and Access Management, (4) Data Protection and Privacy, (5) Security Training, (6) Information Security Continuous Monitoring, (7) Incident Response, and (8) Contingency Planning.

To accomplish our objective, we performed the following procedures:

- reviewed applicable information security regulations, standards, and guidance;
- gained an understanding of information technology security controls by reviewing policies, procedures, and practices that the Department 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 information technology 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' FY 2018 IG FISMA Metrics; and
- compared and tested management, operational, and technical controls based on NIST standards and Department guidance.

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

- performed system-level testing for the Configuration Management, Risk Management, and Contingency Planning metric domains;
- reviewed corrective action plans identified for August 2007 through June 2018;
- identified and verified systems required to use a trusted internet connection;

- tested websites for encryption protocol, masking of personally identifiable information, use of Social Security numbers, and use of website banners;
- tested and reviewed authorized active connections for secure connection protocols;
- reviewed terminated users identified from October 1, 2017 through to April 23, 2018 to determine whether their accounts were terminated;
- identified users who did not take required security training and reviewed all of them to determine whether their accounts were suspended for the months of March and May 2018;
- identified whether operating systems points of contact had access to the Cyber Security Assessment and Management tool;
- reviewed computer security incidents that were reported from October 1, 2017 to July 27, 2018 timeframe;
- performed vulnerability assessment of systems, applications, and infrastructure for Next Generation Data Center's General Support System; Access and Identity Management System; Student Aid Internet Gateway; Postsecondary Educational Participant System; Person Authentication Service; Integrated Student Experience; and Education Security Tracking and Reporting System;
- verified training evidence and completion;
- verified security settings for the Department data protection; and
- observed the all-inclusive EDUCATE disaster recovery exercise.

Sampling Methodology

As of February 2018, the Department identified an inventory of 132 systems that were FISMA reportable and classified as operational. Out of the 132 FISMA reportable systems, 5 systems were classified as high-, 89 as moderate-, and 38 as low-impact systems. Because FSA's transition to the Next Generation Data Center hosting environment was further along than the Department's transition to the new PIVOT hosting environment, we focused our system testing on FSA's Next Generation Data Center environment and selected seven FSA systems. We also chose one Department system that was operational and not impacted by the migration. In making our selection, we considered risk-based characteristics such as system classifications (high, moderate, and low), those systems containing personally identifiable information, and whether systems had been migrated and were fully operational.

The table below lists the judgmentally selected systems, the system's principal office, and the Federal Information Processing Standards Publication 199 potential impact level.[21]

Table 5. Listing of Systems Reviewed

Number	System Name	Principal Office	Impact Level
1	Next Generation Data Center General Support System	FSA	High
2	Access and Identity Management System	FSA	Moderate
3	Person Authentication Service	FSA	Moderate
4	Student Aid Internet Gateway	FSA	Moderate
5	Education Security Tracking and Reporting System	OM	High
6	Postsecondary Educational Participant System	FSA	Moderate
7	Federal Student Aid Information Center	FSA	Moderate
8	Integrated Student Experience	FSA	Moderate

These systems helped us ascertain the security control aspects relating to Configuration Management, Risk Management, and Contingency Planning.[22] In addition, these systems were the focus of our system vulnerability assessment and testing.

During our review of Department controls over its information security program (i.e., FISMA), we also applied the same procedures and analyses in a review of OIG activity. As part of this review, our contractor performed a vulnerability assessment and penetration testing of two OIG systems. Since the OIG is not independent of its own activities, we are not including the results of the review in this report. We did, however,

[21] 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.

[22] 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.

provide the results to OCIO which oversees the Department's information security program. In addition, we reported the results to OIG managers responsible for implementing corrective actions.

In addition to the sample of eight systems, we also used sampling to test certain aspects in the area of security training. Specifically, we identified a total of 247 new users from October 2017 through January 2018. We judgmentally selected a cross-section representation of 12 contractors from each principal office identified as having a new user to determine whether they completed new user security training. Where we relied on judgmental sampling and auditor judgment, we did not project the results from the above samples.

Use of Computer-Processed Data

For this audit, we reviewed the security controls and configuration settings for systems and applications and at the Mid-Atlantic Data Center. We used computer-processed data for the Risk Management, Configuration Management, Identity and Access Management, and Security Training metric domains to support the findings summarized in this report. These data were provided by the Department through self-reporting, or generated through a system where auditors did not have rights to access the system. We performed assessments of the computer-processed data to determine whether the data were reliable for the purpose of our audit. To determine the extent of testing required for the assessment of the data's reliability, we assessed the importance of the data and corroborated it with other types of available evidence. The computer-processed data were verified to source data and tested for accuracy according to relevant system controls until enough information was available to make a reliability determination. For instance, we performed (1) logical tests; (2) comparisons of values to validate a logical or defined correlation; (3) testing for duplicate entries, missing data, and values outside of designated ranges or timeframes; (4) tests using analyzation tools; and (5) comparison of the data with Department scorecards.

We conducted our fieldwork from February 2018 through August 2018, primarily at Department offices in Washington, D.C., and the contractor facility located in Clarksville, Virginia. We conducted an exit conference with Department and FSA officials on October 19, 2018.

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.

Appendix B. New Policy Framework Implementation

In December 2017, the Department initiated a Cybersecurity Framework Alignment for its policy and guidance. As part of the initiative, the Department identified the following challenges it needed to address.

- Information security policies and guidance documents were counterproductive, unstructured, and redundant.
- Current policy and guidance annual review and development cycle were too lengthy. It had an Administrative Communications System process that lasted from 6 to 12 months and had no guarantee of an approval signature.
- Information security policy was a mixture of policy, process, procedures, standards and guidelines that led to communication failures and confusion among employees and contractors.

The Department developed the following solutions to address these challenges:

- a new Information security instruction and standards framework allowing for flexibility;
- a new information security policy.
- breaking down and categorizing the Handbook for Information Assurance Cybersecurity Policy into separate OCIO instructions that are reasonable, enforceable, and aligned to the Cybersecurity Framework under the key Framework Functions—Identify, Protect, Detect, Respond, and Recover;
- a new review workflow and process for newly created instructions that leverage automation to help streamline the review process, and stagger the review dates, so that they are not all due on the same date;
- a new repository for instructions and standards that align with Cybersecurity Framework available through SharePoint and ConnetED; and
- retirement of old policy and guidance documents.

In May 2017, the President signed Executive Order 13800, "Strengthen the Cybersecurity of Federal Networks and Critical Infrastructure," which provided guidance to Federal agencies on updating their critical infrastructure and holding the agency accountable for managing the network enterprise. OMB also directed Federal Agencies with memorandum 17-25, “Reporting Guidance for Executive Order on Strengthening the Cybersecurity Federal Networks and Critical Infrastructure,” to align with the NIST Cybersecurity Framework.

The Department and FSA are in the process of implementing a new policy framework in alignment with the NIST Cybersecurity Framework and the Executive Order M-17-25. In past FISMA audits, we reported findings regarding Department and FSA outdated policy, procedures, and guidance. We found that the Department’s Administrative Communications System process presented many challenges to updating cybersecurity policy and guidance on its website. To address this challenge, the Department hired an individual responsible for providing updated guidance and maintenance of the website.

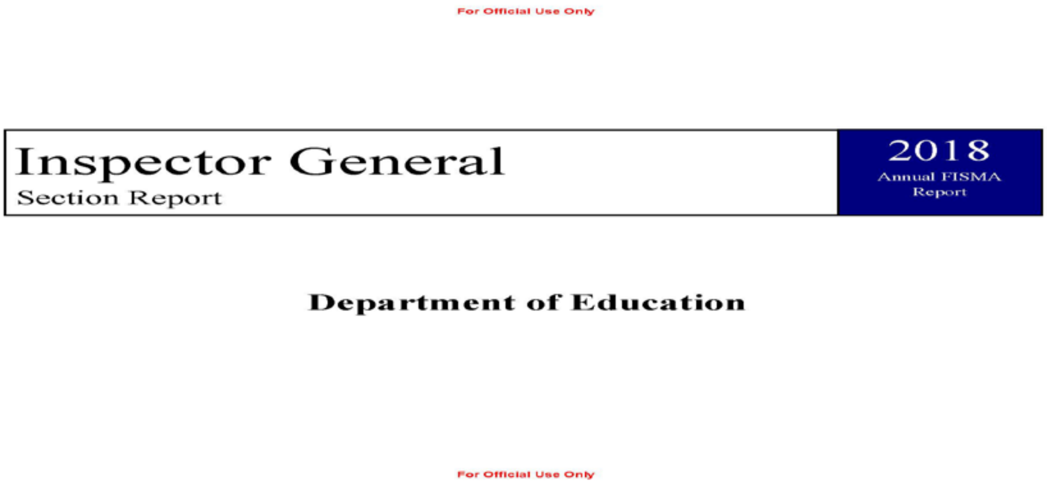
One of the first steps in this process was to establish a new policy framework and update the current cybersecurity policy, Handbook OCIO-01, “Information Assurance Cybersecurity Policy.” The goal of this update was to help retire old policies and guidance documents. The new policy framework will consist of three tiers that include (1) Policy/Directives, (2) Instructions/Standards, and (3) Process, Procedures and Guidelines. The framework will also include the core functions of Identify, Protect, Detect, and Respond and Recover. Consistent with OCIO-01, the updated policy will be the overarching policy that will designate roles and responsibility and information classification and protection.

In July 2018, the Department released a draft of OCIO: 3-112, “Cybersecurity Policy,” that will supersede OCIO-01. In August 2018, it was officially published and is expected to be implemented on October 1, 2018. The purpose of OCIO 3-112 is to provide direction to all Department employees, contractors, and any individual who receives authorization to access Department data, information technology systems, or systems maintained on behalf of the Department to ensure the confidentiality, integrity and availability of information and systems. The Department will communicate this new policy to all stakeholders by including a set of instructional polices that will align to the Executive Order M-17-25. The instructional policies will address the security controls within each of the core functions.

The Department demonstrated that it engaged in updating guidance that will align with the NIST Cybersecurity Framework and that will provide stakeholders with instructions on protecting the Department and FSA information systems and data. We believe that if OCIO continues to incorporate the NIST Cybersecurity Framework into its policies and procedures and strengthen its current policy and procedure process, it will better enable the Department to address current OIG findings and avoid future audit findings.

It will also help the Department and FSA reach Managed and Measureable ratings for all FISMA metric areas to achieve and effective information security program.

Appendix C. CyberScope FY 2018 IG FISMA Metrics



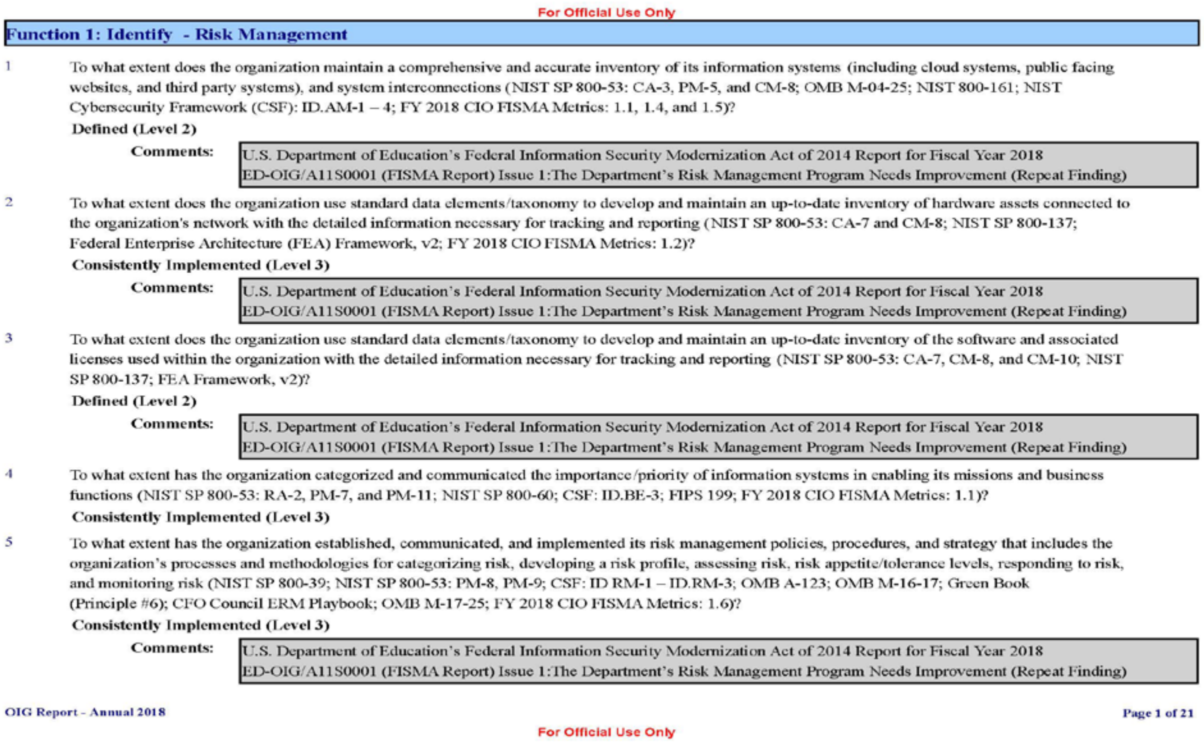
For Official Use Only

Inspector General
Section Report

2018
Annual FISMA
Report

Department of Education

For Official Use Only



For Official Use Only

Function 1: Identify - Risk Management

1 To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third party systems), and system interconnections (NIST SP 800-53: CA-3, PM-5, and CM-8; OMB M-04-25; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2018 CIO FISMA Metrics: 1.1, 1.4, and 1.5)?

Defined (Level 2)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2018 ED-OIG/A11S0001 (FISMA Report) Issue 1:The Department's Risk Management Program Needs Improvement (Repeat Finding)

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; FY 2018 CIO FISMA Metrics: 1.2)?

Consistently Implemented (Level 3)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2018 ED-OIG/A11S0001 (FISMA Report) Issue 1:The Department's Risk Management Program Needs Improvement (Repeat Finding)

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)?

Defined (Level 2)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2018 ED-OIG/A11S0001 (FISMA Report) Issue 1:The Department's Risk Management Program Needs Improvement (Repeat Finding)

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; FIPS 199; FY 2018 CIO FISMA Metrics: 1.1)?

Consistently Implemented (Level 3)

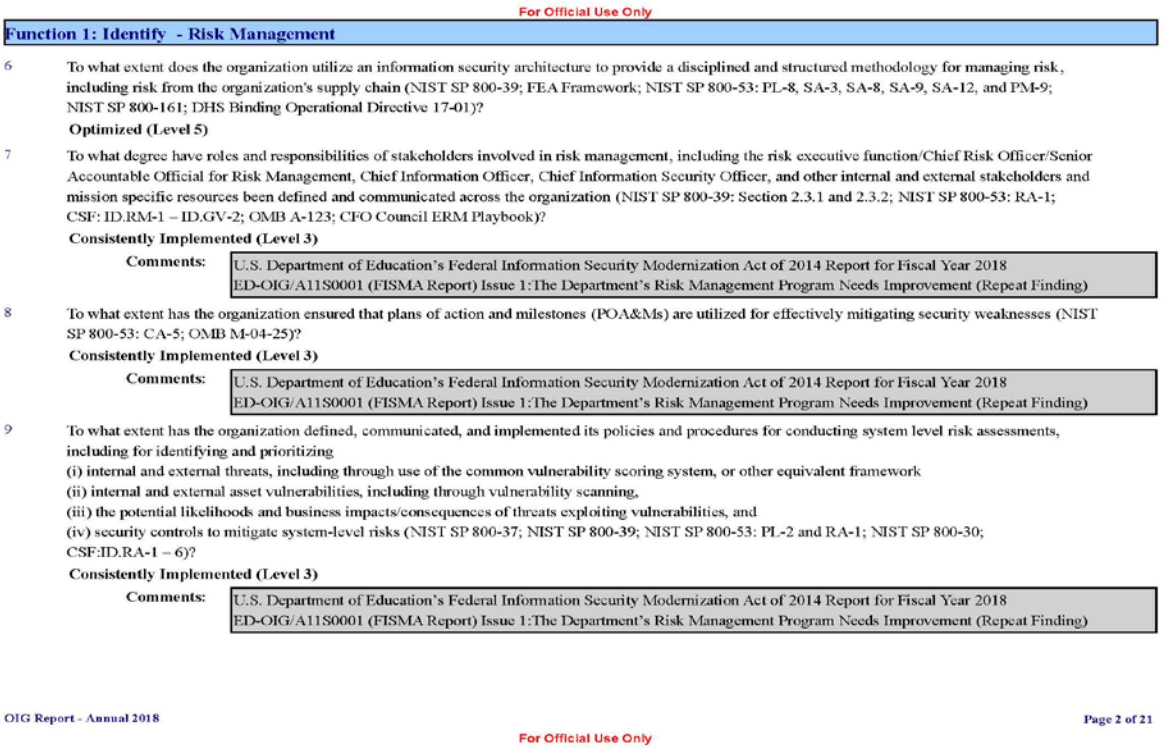
5 To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy that includes the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk (NIST SP 800-39; NIST SP 800-53: PM-8, PM-9; CSF: ID RM-1 – ID.RM-3; OMB A-123; OMB M-16-17; Green Book (Principle #6); CFO Council ERM Playbook; OMB M-17-25; FY 2018 CIO FISMA Metrics: 1.6)?

Consistently Implemented (Level 3)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2018 ED-OIG/A11S0001 (FISMA Report) Issue 1:The Department's Risk Management Program Needs Improvement (Repeat Finding)

OIG Report - Annual 2018 Page 1 of 21

For Official Use Only



Function 1: Identify - Risk Management

6 To what extent does the organization utilize an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain (NIST SP 800-39; FEA Framework; NIST SP 800-53: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-161; DHS Binding Operational Directive 17-01)?

Optimized (Level 5)

7 To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer/Senior Accountable Official for Risk Management, 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 SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2; OMB A-123; CFO Council ERM Playbook)?

Consistently Implemented (Level 3)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2018
ED-OIG/A11S0001 (FISMA Report) Issue 1:The Department's Risk Management Program Needs Improvement (Repeat Finding)

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)?

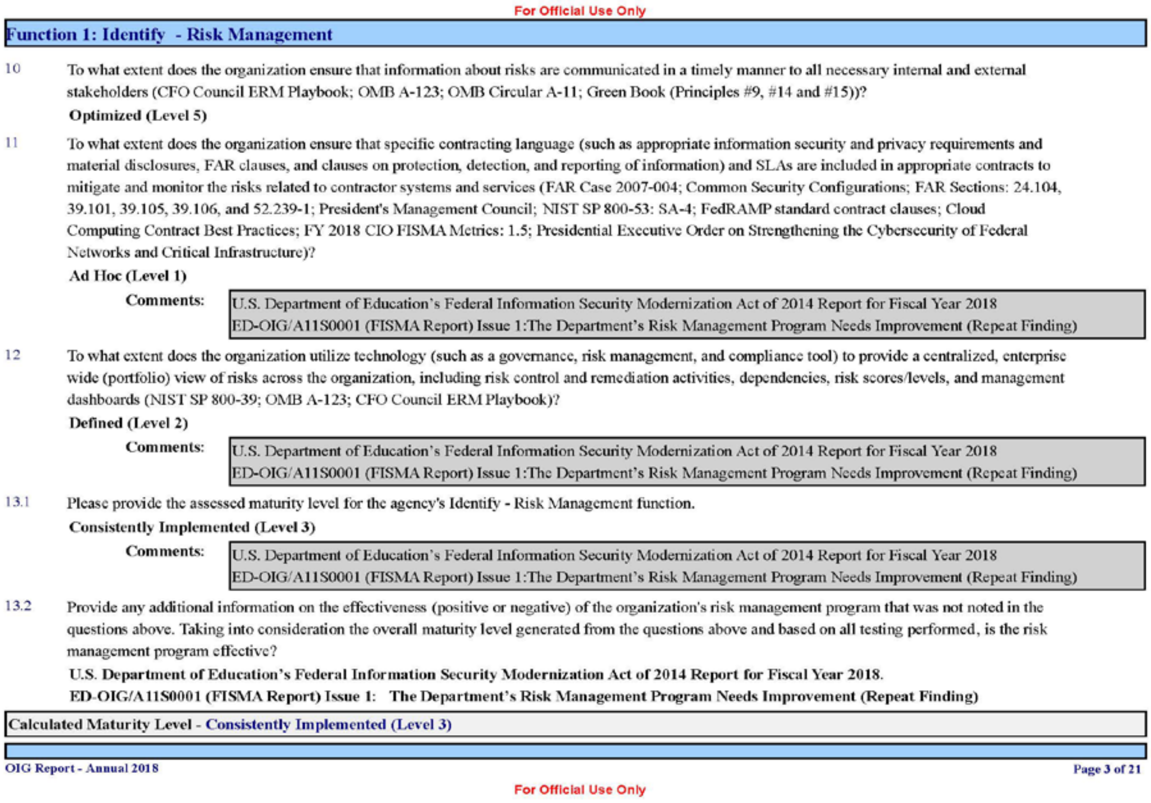
Consistently Implemented (Level 3)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2018
ED-OIG/A11S0001 (FISMA Report) Issue 1:The Department's Risk Management Program Needs Improvement (Repeat Finding)

9 To what extent has the organization defined, communicated, and implemented its policies and procedures for conducting system level risk assessments, including for identifying and prioritizing
(i) internal and external threats, including through use of the common vulnerability scoring system, or other equivalent framework
(ii) internal and external asset vulnerabilities, including through vulnerability scanning,
(iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities, and
(iv) security controls to mitigate system-level risks (NIST SP 800-37; NIST SP 800-39; NIST SP 800-53: PL-2 and RA-1; NIST SP 800-30; CSF:ID.RA-1 – 6)?

Consistently Implemented (Level 3)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2018
ED-OIG/A11S0001 (FISMA Report) Issue 1:The Department's Risk Management Program Needs Improvement (Repeat Finding)



Function 1: Identify - Risk Management

10 To what extent does the organization ensure that information about risks are communicated in a timely manner to all necessary internal and external stakeholders (CFO Council ERM Playbook; OMB A-123; OMB Circular A-11; Green Book (Principles #9, #14 and #15))?

Optimized (Level 5)

11 To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services (FAR Case 2007-004; Common Security Configurations; FAR Sections: 24.104, 39.101, 39.105, 39.106, and 52.239-1; President's Management Council; NIST SP 800-53: SA-4; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; FY 2018 CIO FISMA Metrics: 1.5; Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)?

Ad Hoc (Level 1)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2018
ED-OIG/A11S0001 (FISMA Report) Issue 1:The Department's Risk Management Program Needs Improvement (Repeat Finding)

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

Defined (Level 2)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2018
ED-OIG/A11S0001 (FISMA Report) Issue 1:The Department's Risk Management Program Needs Improvement (Repeat Finding)

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

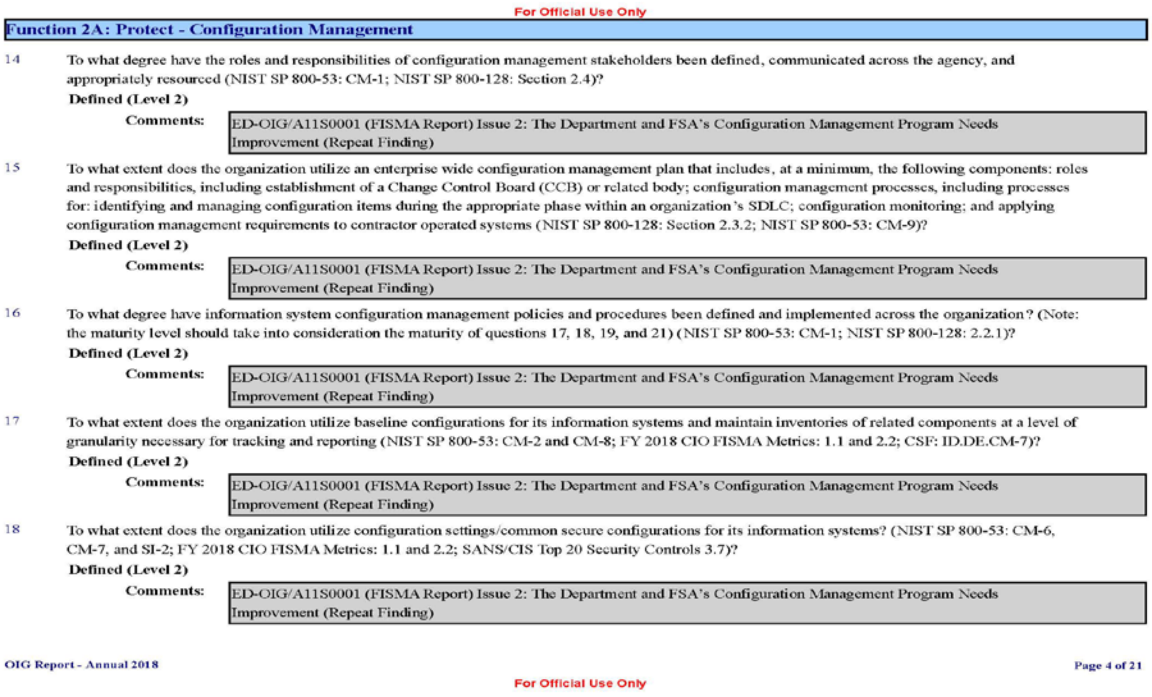
Consistently Implemented (Level 3)

Comments: U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2018
ED-OIG/A11S0001 (FISMA Report) Issue 1:The Department's Risk Management Program Needs Improvement (Repeat Finding)

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

U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2018.
ED-OIG/A11S0001 (FISMA Report) Issue 1: The Department's Risk Management Program Needs Improvement (Repeat Finding)

Calculated Maturity Level - Consistently Implemented (Level 3)



For Official Use Only

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; NIST SP 800-128: Section 2.4)?

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 2: The Department and FSA's Configuration Management Program Needs Improvement (Repeat Finding)

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

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 2: The Department and FSA's Configuration Management Program Needs Improvement (Repeat Finding)

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 SP 800-128: 2.2.1)?

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 2: The Department and FSA's Configuration Management Program Needs Improvement (Repeat Finding)

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 and CM-8; FY 2018 CIO FISMA Metrics: 1.1 and 2.2; CSF: ID.DE.CM-7)?

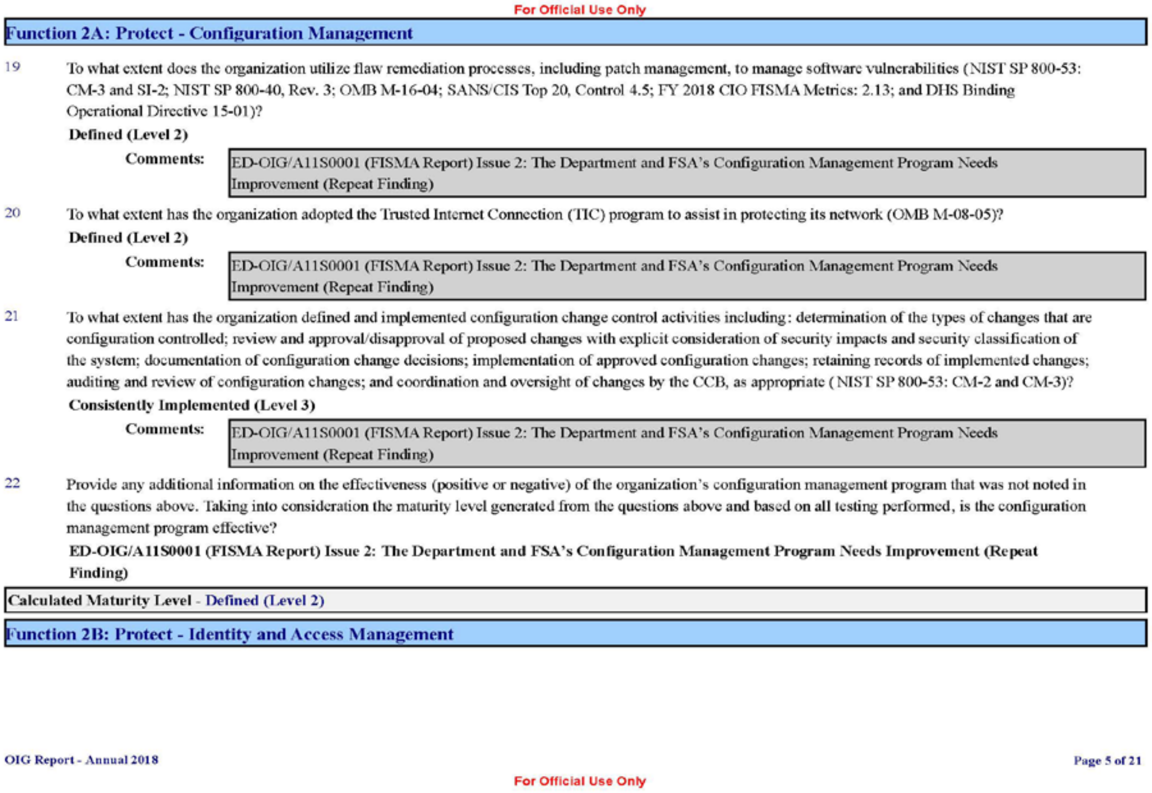
Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 2: The Department and FSA's Configuration Management Program Needs Improvement (Repeat Finding)

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 2018 CIO FISMA Metrics: 1.1 and 2.2; SANS/CIS Top 20 Security Controls 3.7)?

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 2: The Department and FSA's Configuration Management Program Needs Improvement (Repeat Finding)



For Official Use Only

Function 2A: Protect - Configuration Management

19 To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53: CM-3 and SI-2; NIST SP 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20, Control 4.5; FY 2018 CIO FISMA Metrics: 2.13; and DHS Binding Operational Directive 15-01)?

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 2: The Department and FSA's Configuration Management Program Needs Improvement (Repeat Finding)

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

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 2: The Department and FSA's Configuration Management Program Needs Improvement (Repeat Finding)

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

Consistently Implemented (Level 3)

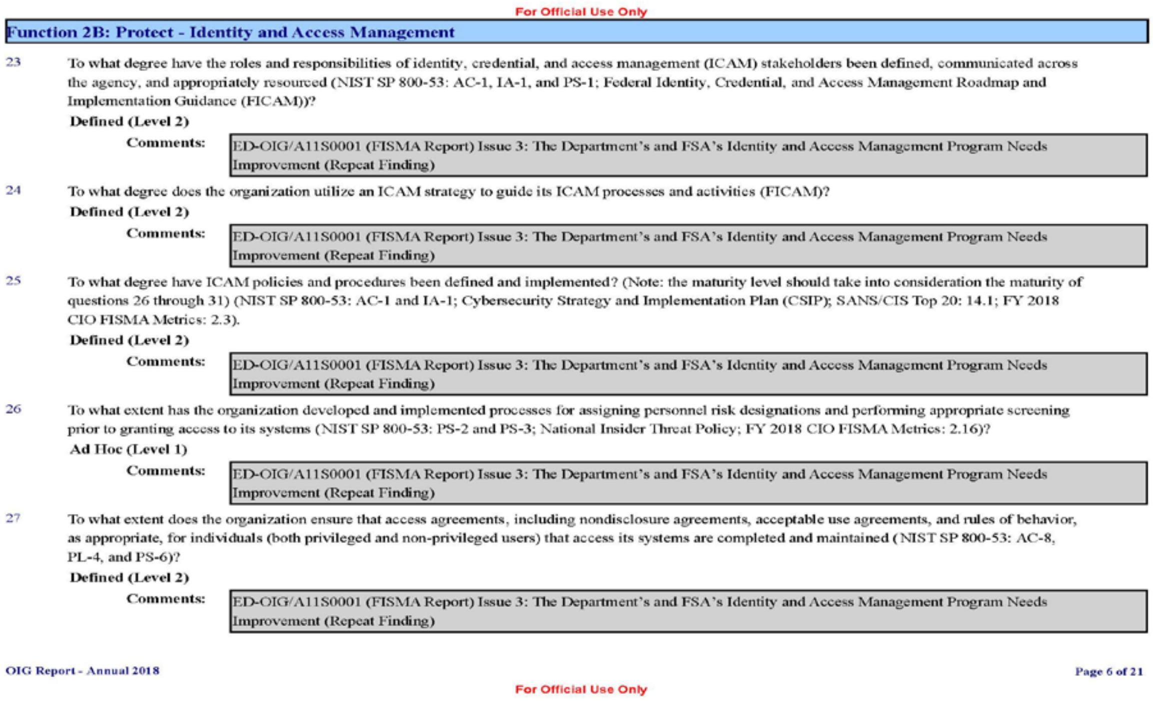
Comments: ED-OIG/A11S0001 (FISMA Report) Issue 2: The Department and FSA's Configuration Management Program Needs Improvement (Repeat Finding)

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?

ED-OIG/A11S0001 (FISMA Report) Issue 2: The Department and FSA's Configuration Management Program Needs Improvement (Repeat Finding)

Calculated Maturity Level - Defined (Level 2)

Function 2B: Protect - Identity and Access Management



For Official Use Only

Function 2B: Protect - Identity and Access Management

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

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 3: The Department's and FSA's Identity and Access Management Program Needs Improvement (Repeat Finding)

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

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 3: The Department's and FSA's Identity and Access Management Program Needs Improvement (Repeat Finding)

25 To what degree have ICAM policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 26 through 31) (NIST SP 800-53: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; FY 2018 CIO FISMA Metrics: 2.3).

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 3: The Department's and FSA's Identity and Access Management Program Needs Improvement (Repeat Finding)

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 and PS-3; National Insider Threat Policy; FY 2018 CIO FISMA Metrics: 2.16)?

Ad Hoc (Level 1)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 3: The Department's and FSA's Identity and Access Management Program Needs Improvement (Repeat Finding)

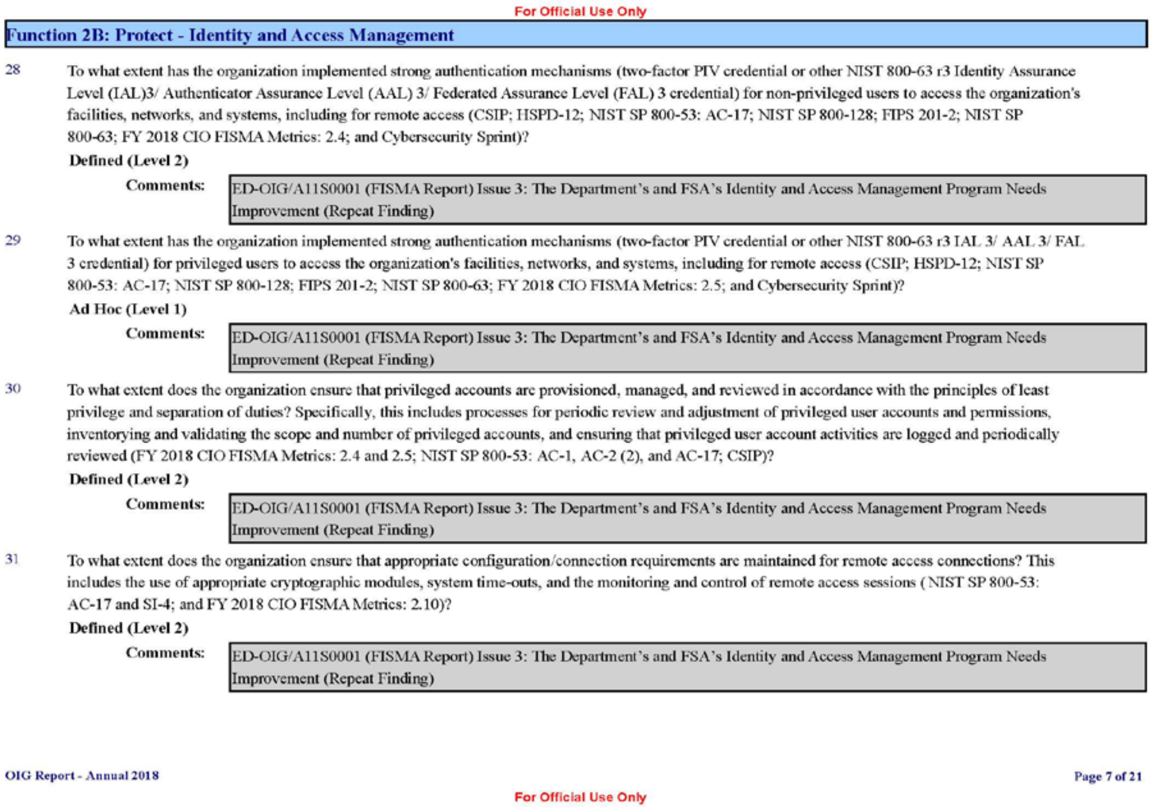
27 To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non-privileged users) that access its systems are completed and maintained (NIST SP 800-53: AC-8, PL-4, and PS-6)?

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 3: The Department's and FSA's Identity and Access Management Program Needs Improvement (Repeat Finding)

OIG Report - Annual 2018 Page 6 of 21

For Official Use Only



For Official Use Only

Function 2B: Protect - Identity and Access Management

28 To what extent has the organization implemented strong authentication mechanisms (two-factor PIV credential or other NIST 800-63 r3 Identity Assurance Level (IAL)3/ Authenticator Assurance Level (AAL) 3/ Federated Assurance Level (FAL) 3 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; FY 2018 CIO FISMA Metrics: 2.4; and Cybersecurity Sprint)?

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 3: The Department's and FSA's Identity and Access Management Program Needs Improvement (Repeat Finding)

29 To what extent has the organization implemented strong authentication mechanisms (two-factor PIV credential or other NIST 800-63 r3 IAL 3/ AAL 3/ FAL 3 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; FY 2018 CIO FISMA Metrics: 2.5; and Cybersecurity Sprint)?

Ad Hoc (Level 1)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 3: The Department's and FSA's Identity and Access Management Program Needs Improvement (Repeat Finding)

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 2018 CIO FISMA Metrics: 2.4 and 2.5; NIST SP 800-53: AC-1, AC-2 (2), and AC-17; CSIP)?

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 3: The Department's and FSA's Identity and Access Management Program Needs Improvement (Repeat Finding)

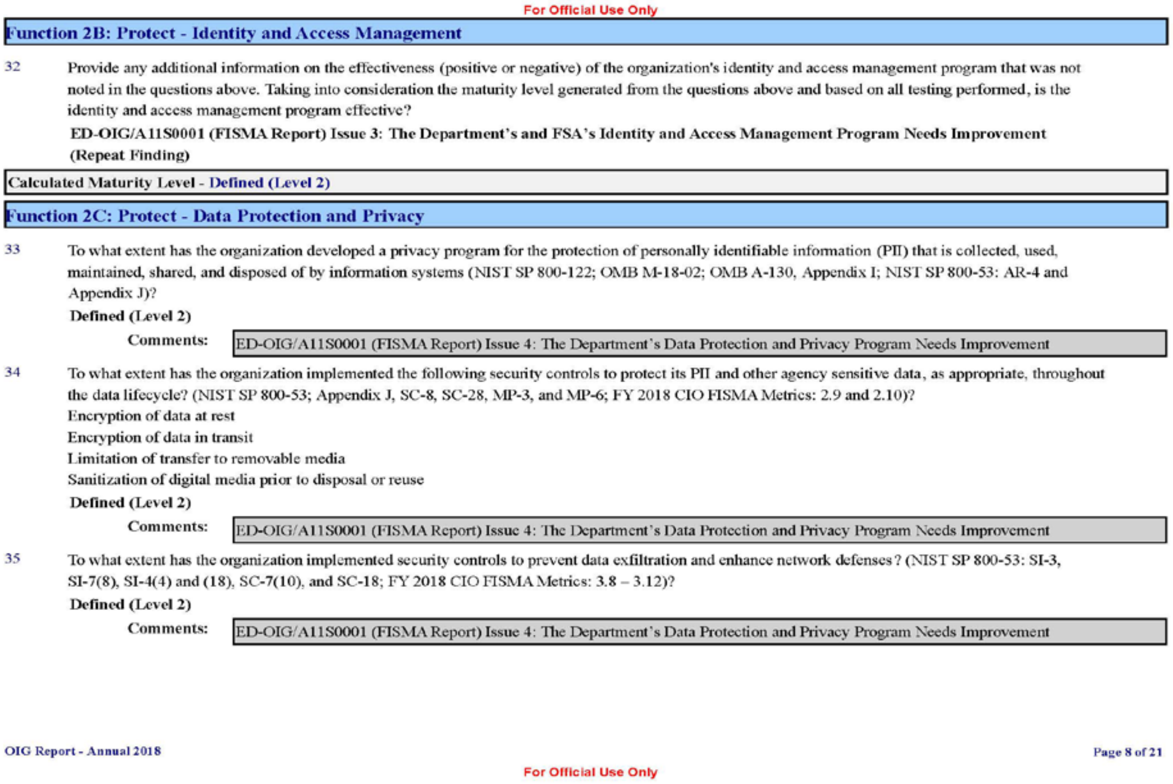
31 To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions (NIST SP 800-53: AC-17 and SI-4; and FY 2018 CIO FISMA Metrics: 2.10)?

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 3: The Department's and FSA's Identity and Access Management Program Needs Improvement (Repeat Finding)

OIG Report - Annual 2018 Page 7 of 21

For Official Use Only



For Official Use Only

Function 2B: Protect - Identity and Access Management

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

ED-OIG/A11S0001 (FISMA Report) Issue 3: The Department's and FSA's Identity and Access Management Program Needs Improvement (Repeat Finding)

Calculated Maturity Level - Defined (Level 2)

Function 2C: Protect - Data Protection and Privacy

33 To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems (NIST SP 800-122; OMB M-18-02; OMB A-130, Appendix I; NIST SP 800-53: AR-4 and Appendix J)?

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 4: The Department's Data Protection and Privacy Program Needs Improvement

34 To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle? (NIST SP 800-53; Appendix J, SC-8, SC-28, MP-3, and MP-6; FY 2018 CIO FISMA Metrics: 2.9 and 2.10)?
Encryption of data at rest
Encryption of data in transit
Limitation of transfer to removable media
Sanitization of digital media prior to disposal or reuse

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 4: The Department's Data Protection and Privacy Program Needs Improvement

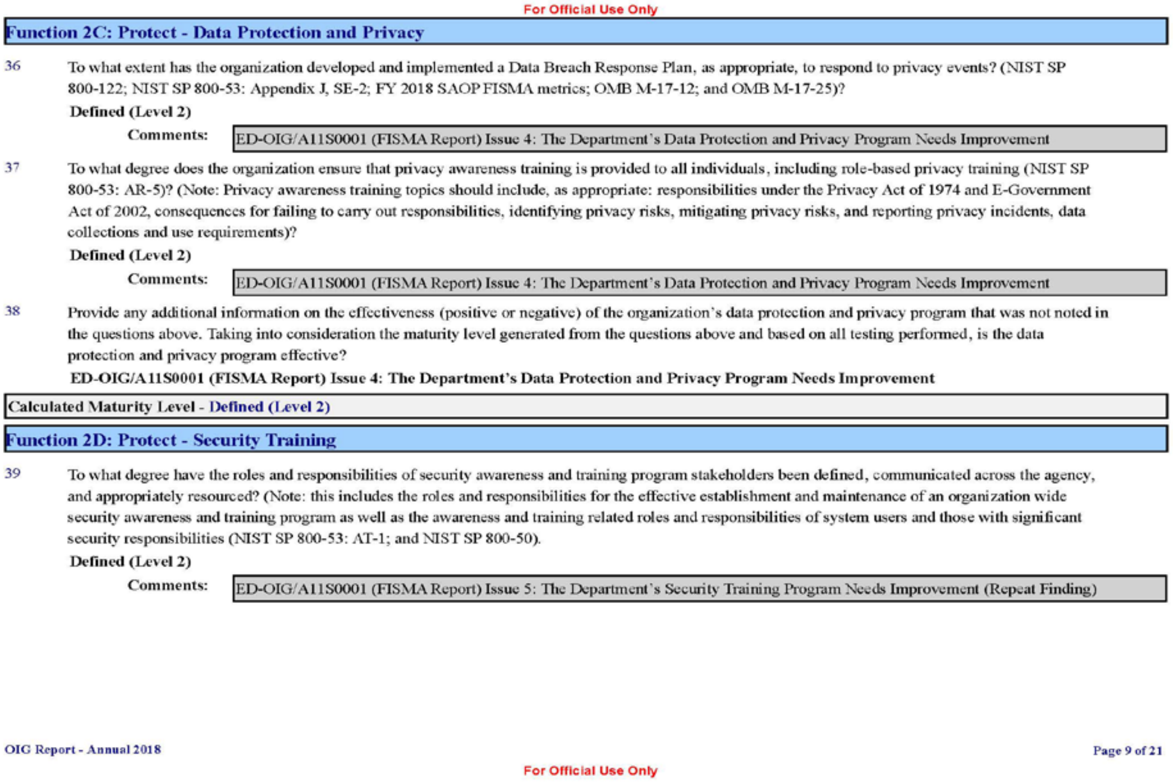
35 To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (NIST SP 800-53: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2018 CIO FISMA Metrics: 3.8 – 3.12)?

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 4: The Department's Data Protection and Privacy Program Needs Improvement

OIG Report - Annual 2018 Page 8 of 21

For Official Use Only



For Official Use Only

Function 2C: Protect - Data Protection and Privacy

36 To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events? (NIST SP 800-122; NIST SP 800-53: Appendix J, SE-2; FY 2018 SAOP FISMA metrics; OMB M-17-12; and OMB M-17-25)?

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 4: The Department's Data Protection and Privacy Program Needs Improvement

37 To what degree does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training (NIST SP 800-53: AR-5)? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements)?

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 4: The Department's Data Protection and Privacy Program Needs Improvement

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

ED-OIG/A11S0001 (FISMA Report) Issue 4: The Department's Data Protection and Privacy Program Needs Improvement

Calculated Maturity Level - Defined (Level 2)

Function 2D: Protect - Security Training

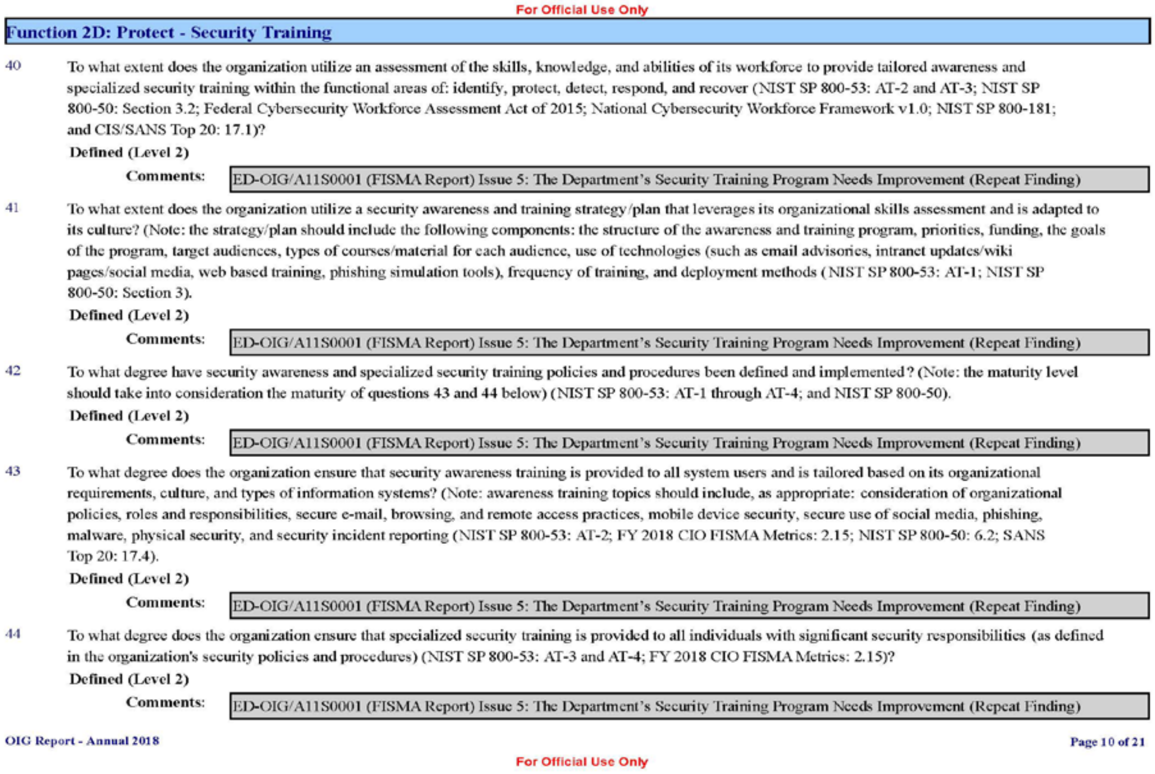
39 To what degree have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated across the agency, and appropriately resourced? (Note: this includes the roles and responsibilities for the effective establishment and maintenance of an organization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

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 5: The Department's Security Training Program Needs Improvement (Repeat Finding)

OIG Report - Annual 2018 Page 9 of 21

For Official Use Only



For Official Use Only

Function 2D: Protect - Security Training

40 To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover (NIST SP 800-53: AT-2 and AT-3; NIST SP 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; and CIS/SANS Top 20: 17.1)?

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 5: The Department's Security Training Program Needs Improvement (Repeat Finding)

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

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 5: The Department's Security Training Program Needs Improvement (Repeat Finding)

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

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 5: The Department's Security Training Program Needs Improvement (Repeat Finding)

43 To what degree does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST SP 800-53: AT-2; FY 2018 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; SANS Top 20: 17.4).

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 5: The Department's Security Training Program Needs Improvement (Repeat Finding)

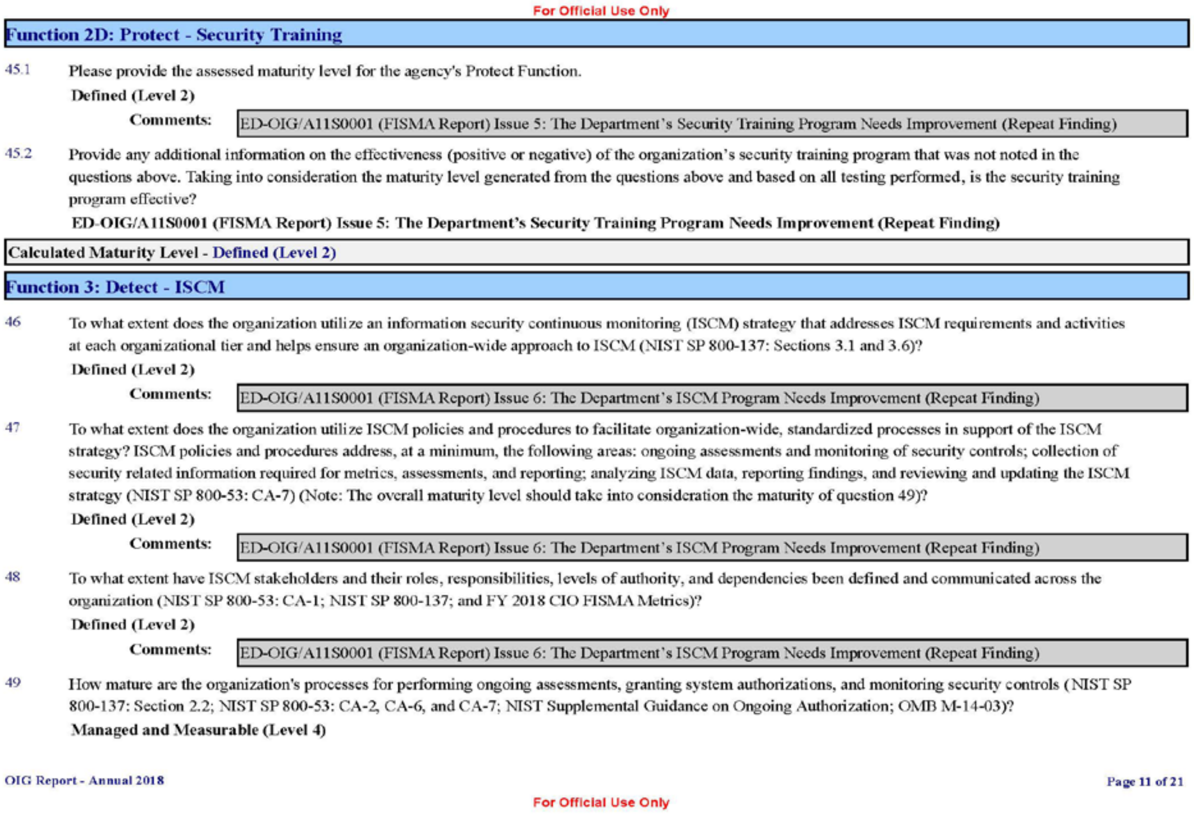
44 To what degree does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures) (NIST SP 800-53: AT-3 and AT-4; FY 2018 CIO FISMA Metrics: 2.15)?

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 5: The Department's Security Training Program Needs Improvement (Repeat Finding)

OIG Report - Annual 2018 Page 10 of 21

For Official Use Only



For Official Use Only

Function 2D: Protect - Security Training

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

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 5: The Department's Security Training Program Needs Improvement (Repeat Finding)

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

ED-OIG/A11S0001 (FISMA Report) Issue 5: The Department's Security Training Program Needs Improvement (Repeat Finding)

Calculated Maturity Level - Defined (Level 2)

Function 3: Detect - ISCM

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

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 6: The Department's ISCM Program Needs Improvement (Repeat Finding)

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

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 6: The Department's ISCM Program Needs Improvement (Repeat Finding)

48 To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53: CA-1; NIST SP 800-137; and FY 2018 CIO FISMA Metrics)?

Defined (Level 2)

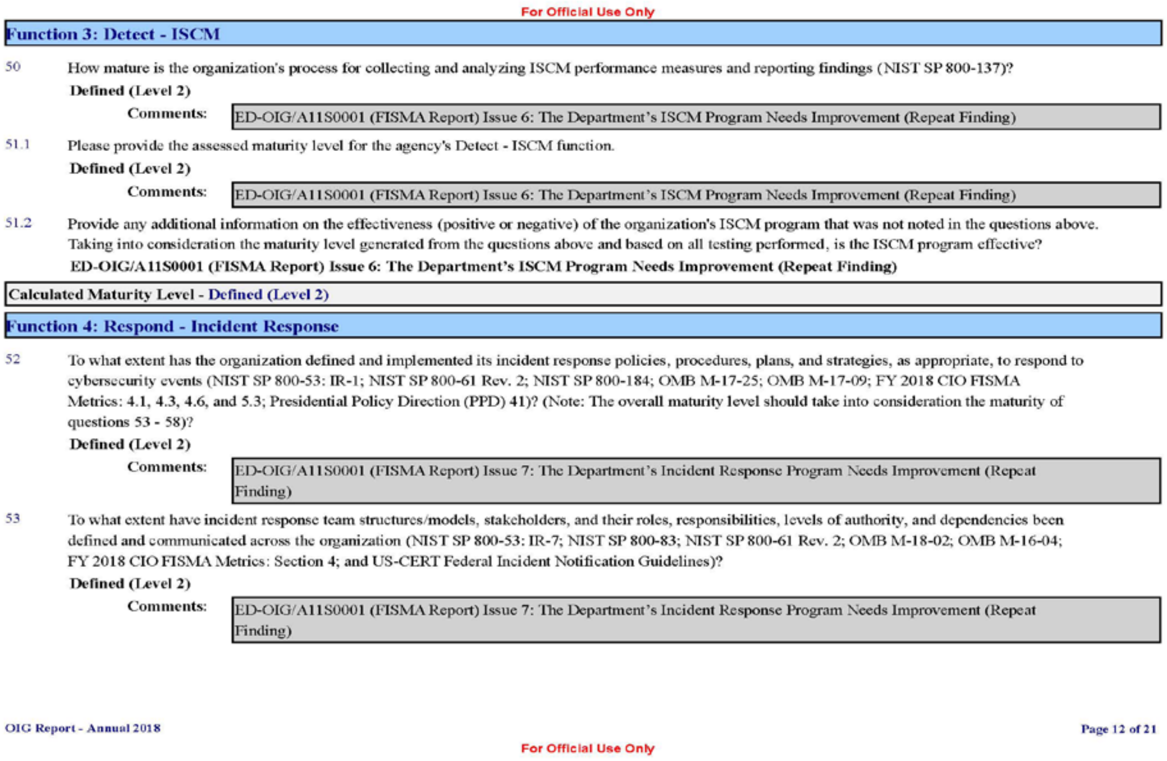
Comments: ED-OIG/A11S0001 (FISMA Report) Issue 6: The Department's ISCM Program Needs Improvement (Repeat Finding)

49 How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls (NIST SP 800-137: Section 2.2; NIST SP 800-53: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; OMB M-14-03)?

Managed and Measurable (Level 4)

OIG Report - Annual 2018 Page 11 of 21

For Official Use Only



Function 3: Detect - ISCM

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

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 6: The Department's ISCM Program Needs Improvement (Repeat Finding)

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

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 6: The Department's ISCM Program Needs Improvement (Repeat Finding)

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

ED-OIG/A11S0001 (FISMA Report) Issue 6: The Department's ISCM Program Needs Improvement (Repeat Finding)

Calculated Maturity Level - Defined (Level 2)

Function 4: Respond - Incident Response

52 To what extent has the organization defined and implemented its incident response policies, procedures, plans, and strategies, as appropriate, to respond to cybersecurity events (NIST SP 800-53: IR-1; NIST SP 800-61 Rev. 2; NIST SP 800-184; OMB M-17-25; OMB M-17-09; FY 2018 CIO FISMA Metrics: 4.1, 4.3, 4.6, and 5.3; Presidential Policy Direction (PPD) 41)? (Note: The overall maturity level should take into consideration the maturity of questions 53 - 58)?

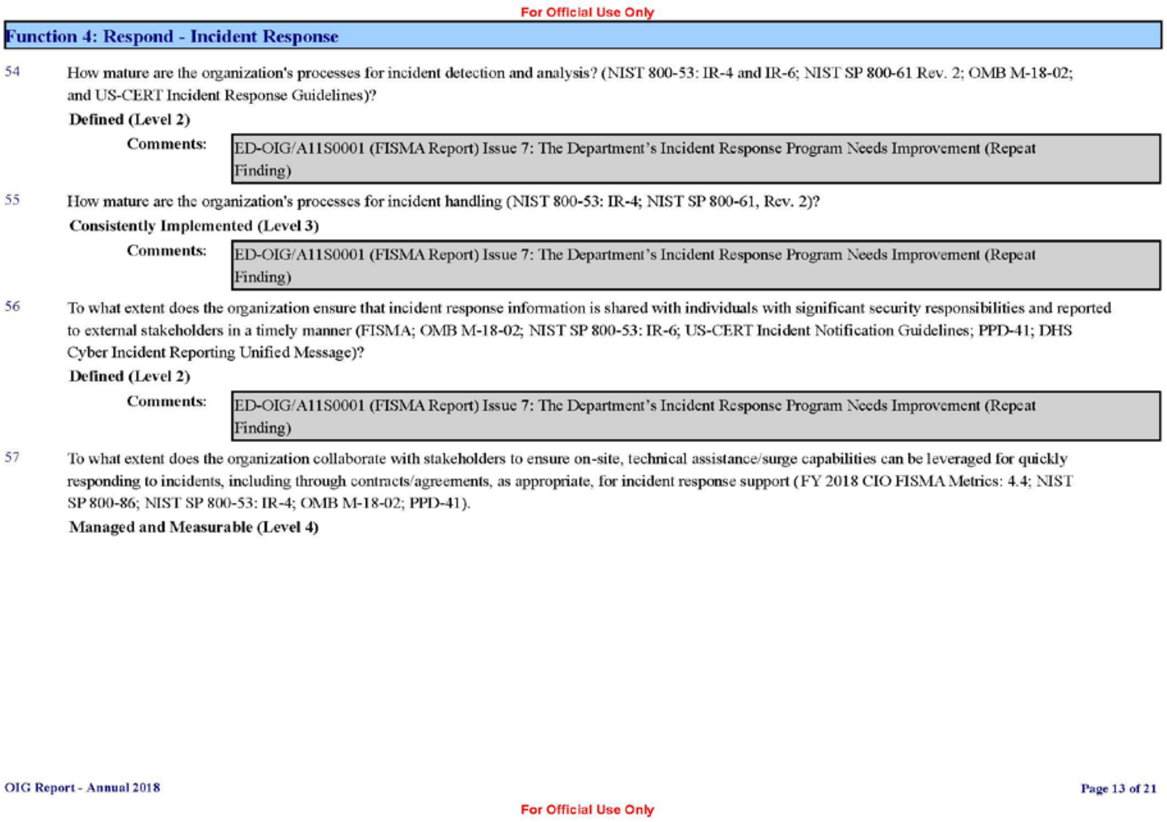
Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 7: The Department's Incident Response Program Needs Improvement (Repeat Finding)

53 To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-18-02; OMB M-16-04; FY 2018 CIO FISMA Metrics: Section 4; and US-CERT Federal Incident Notification Guidelines)?

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 7: The Department's Incident Response Program Needs Improvement (Repeat Finding)



Function 4: Respond - Incident Response

54 How mature are the organization's processes for incident detection and analysis? (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; OMB M-18-02; and US-CERT Incident Response Guidelines)?

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 7: The Department's Incident Response Program Needs Improvement (Repeat Finding)

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

Consistently Implemented (Level 3)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 7: The Department's Incident Response Program Needs Improvement (Repeat Finding)

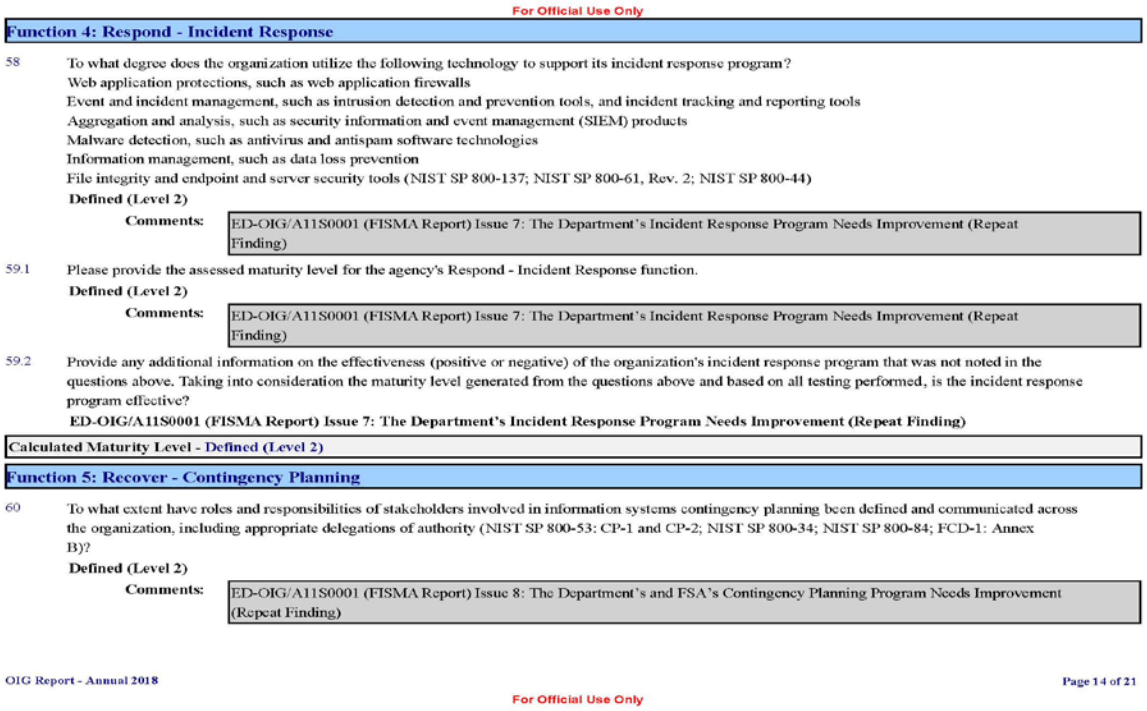
56 To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-18-02; NIST SP 800-53: IR-6; US-CERT Incident Notification Guidelines; PPD-41; DHS Cyber Incident Reporting Unified Message)?

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 7: The Department's Incident Response Program Needs Improvement (Repeat Finding)

57 To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support (FY 2018 CIO FISMA Metrics: 4.4; NIST SP 800-86; NIST SP 800-53: IR-4; OMB M-18-02; PPD-41).

Managed and Measurable (Level 4)



Function 4: Respond - Incident Response

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

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 7: The Department's Incident Response Program Needs Improvement (Repeat Finding)

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

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 7: The Department's Incident Response Program Needs Improvement (Repeat Finding)

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

ED-OIG/A11S0001 (FISMA Report) Issue 7: The Department's Incident Response Program Needs Improvement (Repeat Finding)

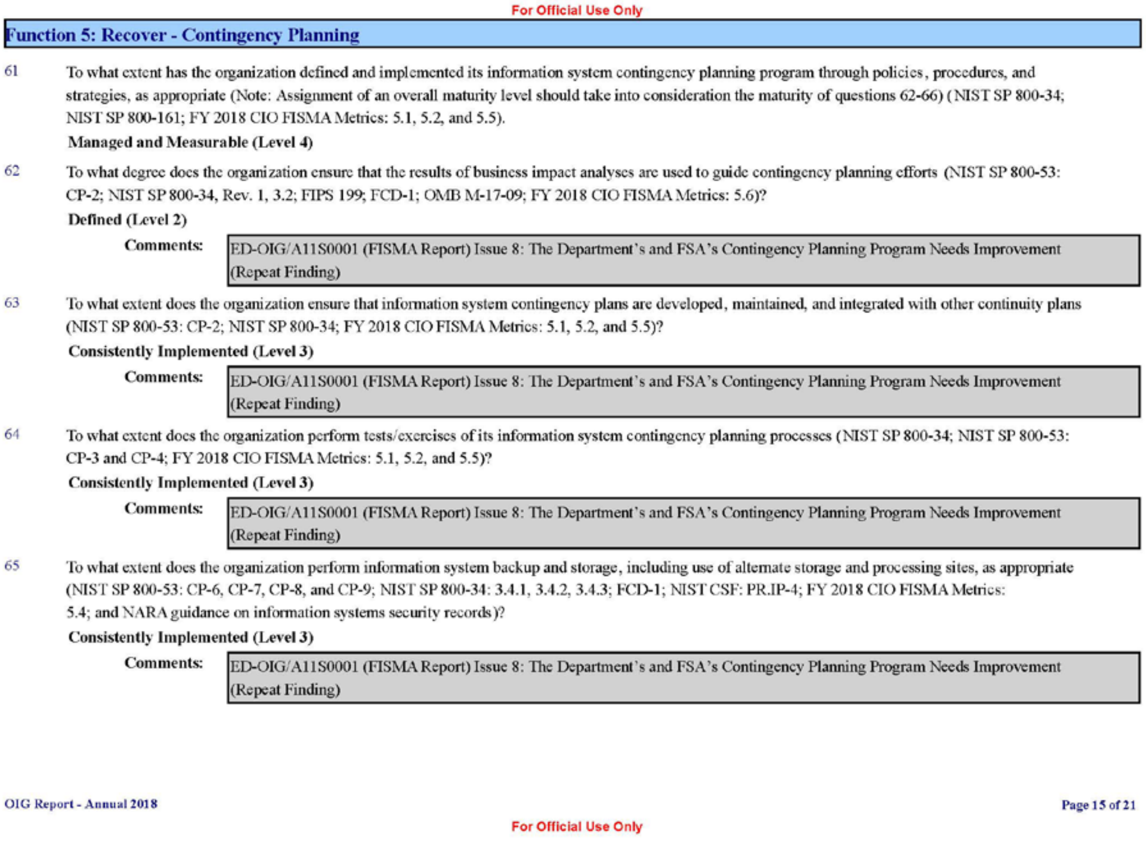
Calculated Maturity Level - Defined (Level 2)

Function 5: Recover - Contingency Planning

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

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 8: The Department's and FSA's Contingency Planning Program Needs Improvement (Repeat Finding)



Function 5: Recover - Contingency Planning

61 To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and strategies, as appropriate (Note: Assignment of an overall maturity level should take into consideration the maturity of questions 62-66) (NIST SP 800-34; NIST SP 800-161; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5).

Managed and Measurable (Level 4)

62 To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST SP 800-53: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-17-09; FY 2018 CIO FISMA Metrics: 5.6)?

Defined (Level 2)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 8: The Department's and FSA's Contingency Planning Program Needs Improvement (Repeat Finding)

63 To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST SP 800-53: CP-2; NIST SP 800-34; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5)?

Consistently Implemented (Level 3)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 8: The Department's and FSA's Contingency Planning Program Needs Improvement (Repeat Finding)

64 To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST SP 800-34; NIST SP 800-53: CP-3 and CP-4; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5)?

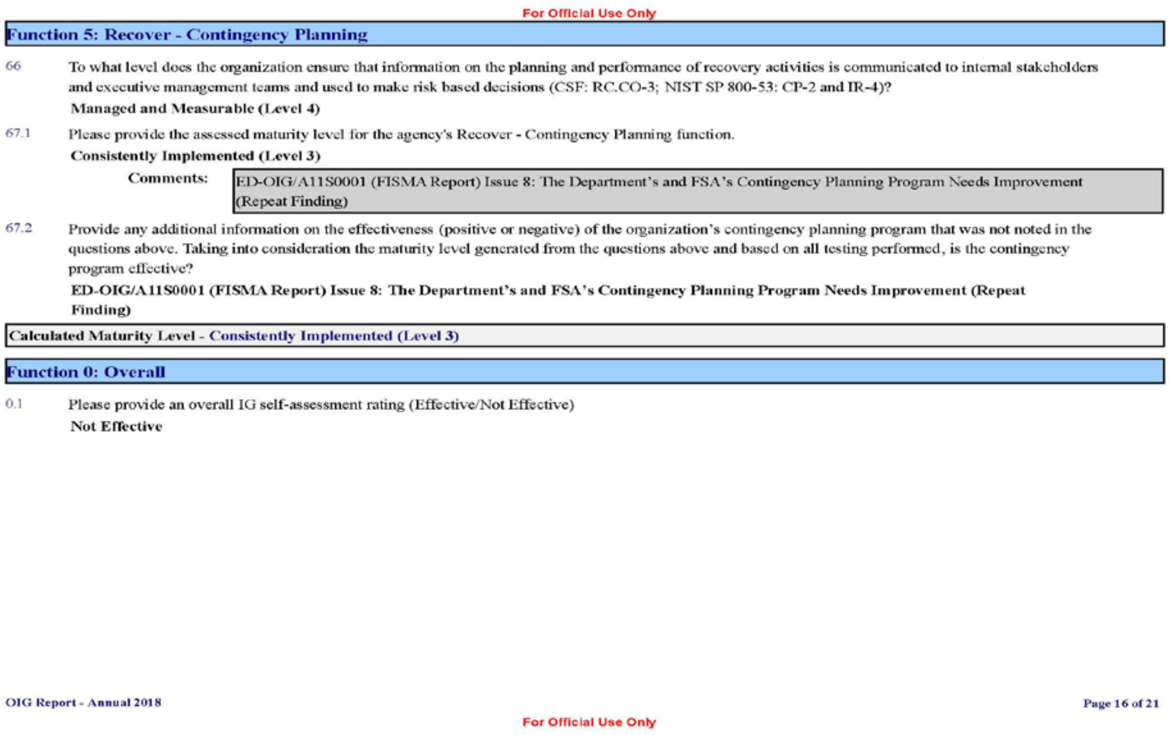
Consistently Implemented (Level 3)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 8: The Department's and FSA's Contingency Planning Program Needs Improvement (Repeat Finding)

65 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST SP 800-53: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD-1; NIST CSF: PR.IP-4; FY 2018 CIO FISMA Metrics: 5.4; and NARA guidance on information systems security records)?

Consistently Implemented (Level 3)

Comments: ED-OIG/A11S0001 (FISMA Report) Issue 8: The Department's and FSA's Contingency Planning Program Needs Improvement (Repeat Finding)



Function 5: Recover - Contingency Planning

66 To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk based decisions (CSF: RC.CO-3; NIST SP 800-53: CP-2 and IR-4)?

Managed and Measurable (Level 4)

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

Consistently Implemented (Level 3)

Comments:	ED-OIG/A11S0001 (FISMA Report) Issue 8: The Department's and FSA's Contingency Planning Program Needs Improvement (Repeat Finding)

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

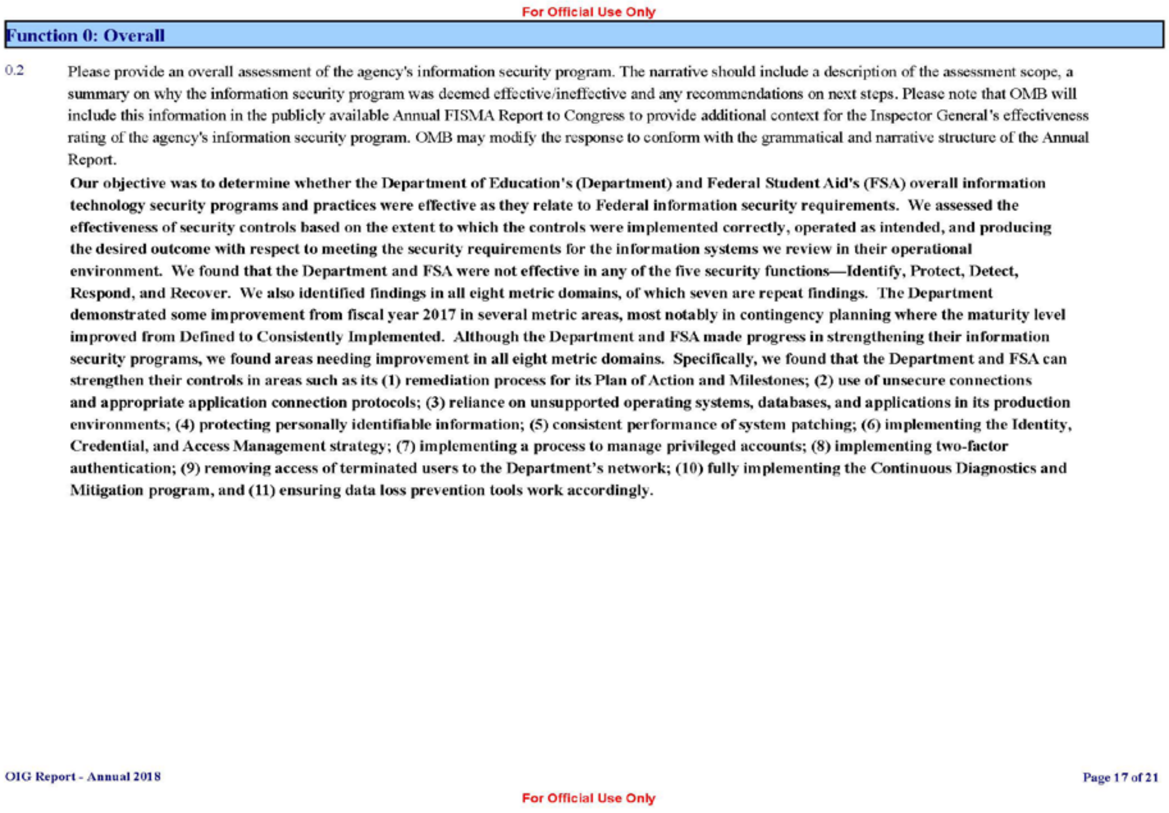
ED-OIG/A11S0001 (FISMA Report) Issue 8: The Department's and FSA's Contingency Planning Program Needs Improvement (Repeat Finding)

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 0: Overall

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

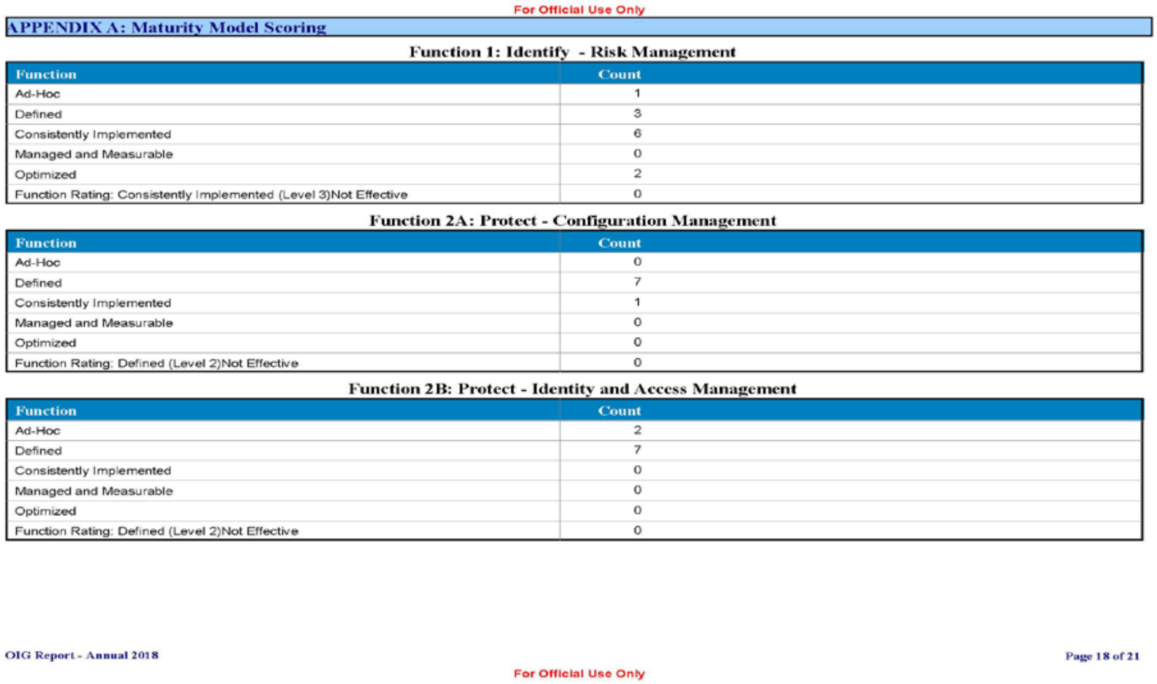
Not Effective



Function 0: Overall

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

Our objective was to determine whether the Department of Education's (Department) and Federal Student Aid's (FSA) overall information technology security programs and practices were effective as they relate to Federal information security requirements. We assessed the effectiveness of security controls based on the extent to which the controls were implemented correctly, operated as intended, and producing the desired outcome with respect to meeting the security requirements for the information systems we review in their operational environment. We found that the Department and FSA were not effective in any of the five security functions—Identify, Protect, Detect, Respond, and Recover. We also identified findings in all eight metric domains, of which seven are repeat findings. The Department demonstrated some improvement from fiscal year 2017 in several metric areas, most notably in contingency planning where the maturity level improved from Defined to Consistently Implemented. Although the Department and FSA made progress in strengthening their information security programs, we found areas needing improvement in all eight metric domains. Specifically, we found that the Department and FSA can strengthen their controls in areas such as its (1) remediation process for its Plan of Action and Milestones; (2) use of unsecure connections and appropriate application connection protocols; (3) reliance on unsupported operating systems, databases, and applications in its production environments; (4) protecting personally identifiable information; (5) consistent performance of system patching; (6) implementing the Identity, Credential, and Access Management strategy; (7) implementing a process to manage privileged accounts; (8) implementing two-factor authentication; (9) removing access of terminated users to the Department's network; (10) fully implementing the Continuous Diagnostics and Mitigation program, and (11) ensuring data loss prevention tools work accordingly.



For Official Use Only

APPENDIX A: Maturity Model Scoring

Function 1: Identify - Risk Management

Function	Count
Ad-Hoc	1
Defined	3
Consistently Implemented	6
Managed and Measurable	0
Optimized	2
Function Rating: Consistently Implemented (Level 3)Not Effective	0

Function 2A: Protect - Configuration Management

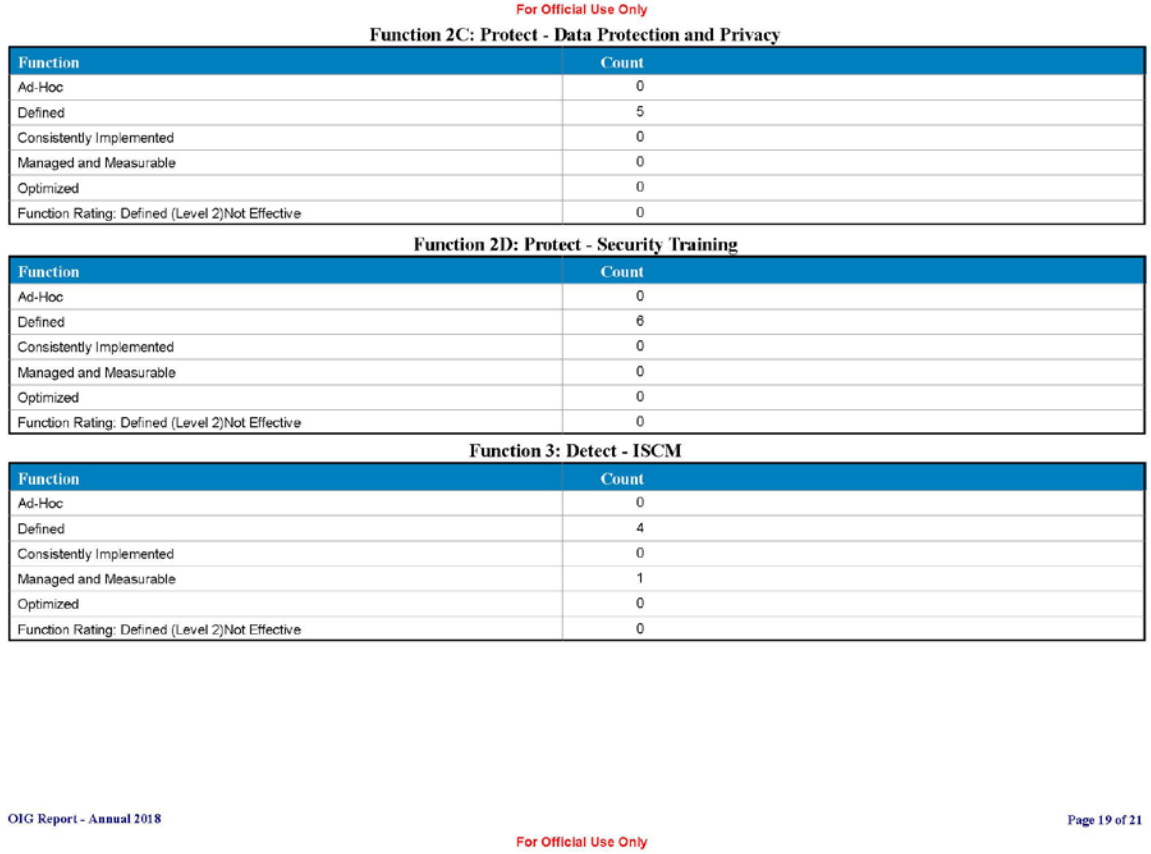
Function	Count
Ad-Hoc	0
Defined	7
Consistently Implemented	1
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)Not Effective	0

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)Not Effective	0

OIG Report - Annual 2018 Page 18 of 21

For Official Use Only



For Official Use Only

Function 2C: Protect - Data Protection and Privacy

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

Function 2D: Protect - Security Training

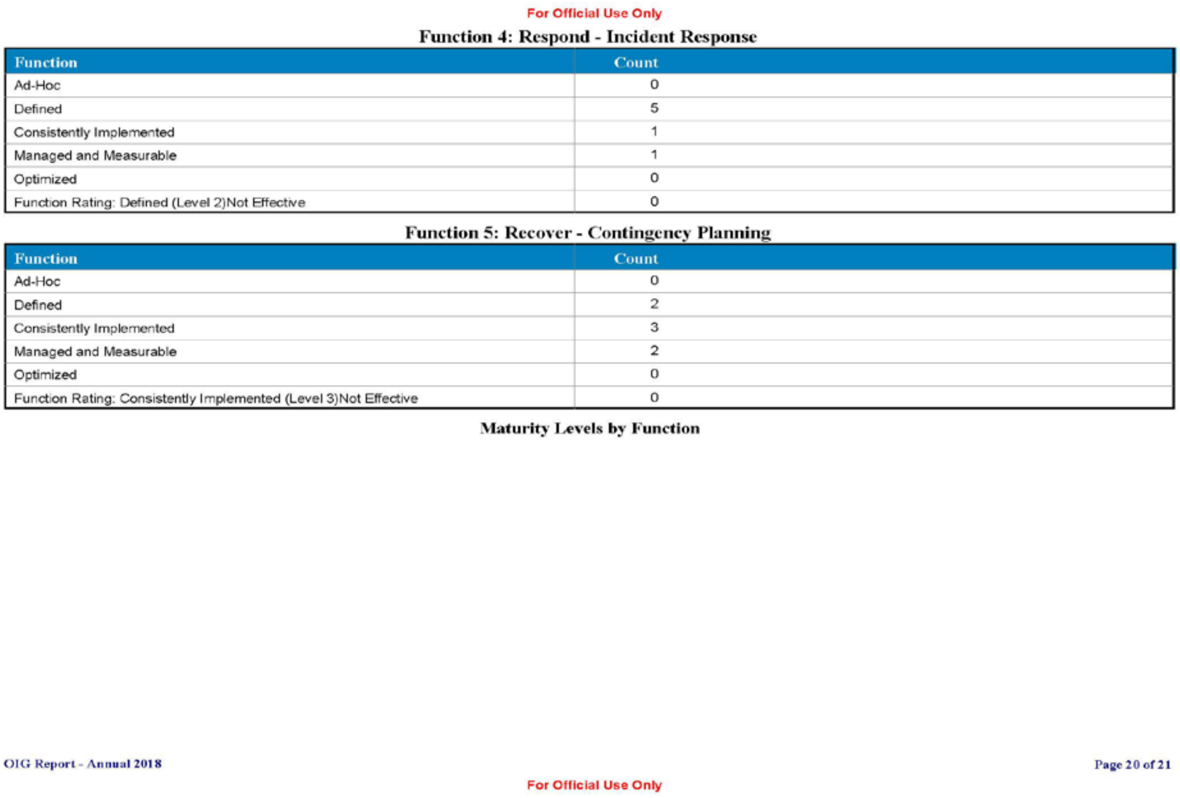
Function	Count
Ad-Hoc	0
Defined	6
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)Not Effective	0

Function 3: Detect - ISCM

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

OIG Report - Annual 2018 Page 19 of 21

For Official Use Only



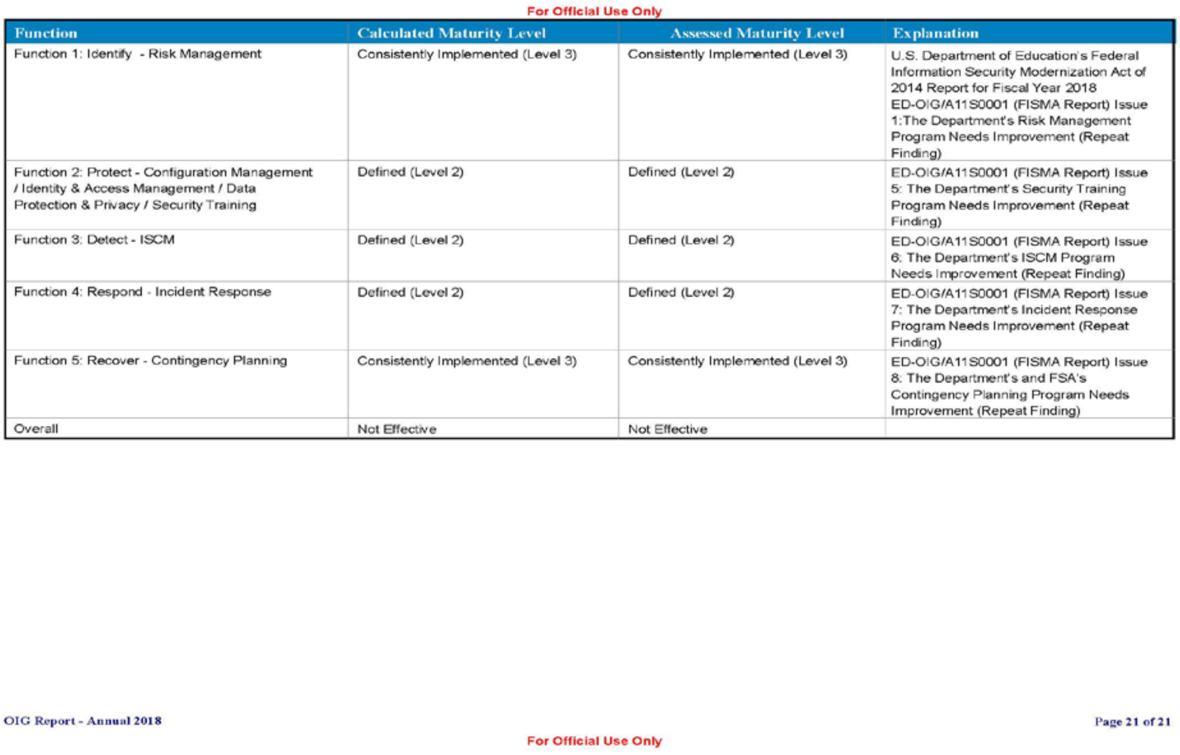
Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	5
Consistently Implemented	1
Managed and Measurable	1
Optimized	0
Function Rating: Defined (Level 2)Not Effective	0

Function 5: Recover - Contingency Planning

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

Maturity Levels by Function

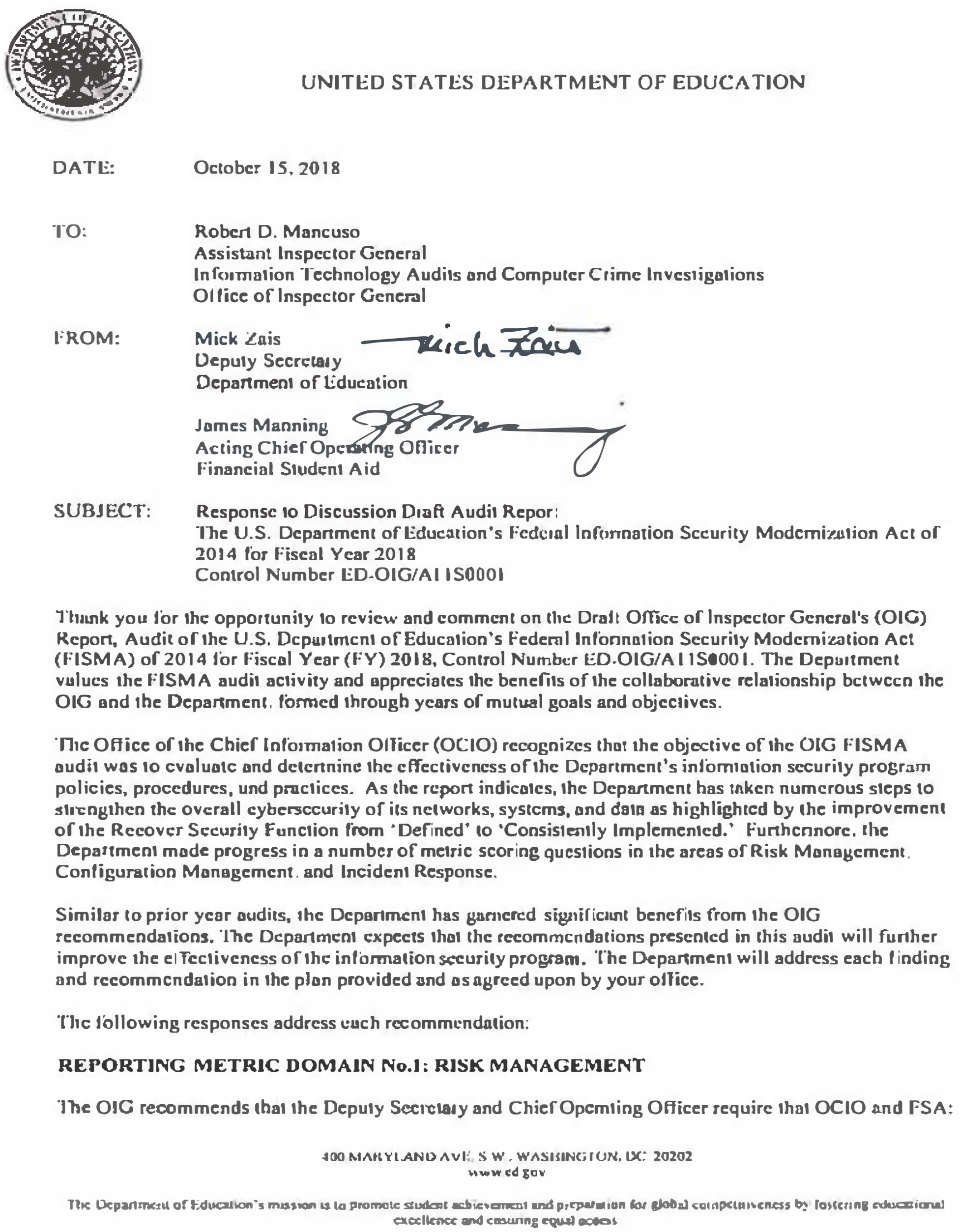


Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report for Fiscal Year 2018 ED-OIG/A11S0001 (FISMA Report) Issue 1:The Department's Risk Management Program Needs Improvement (Repeat Finding)
Function 2: Protect - Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training	Defined (Level 2)	Defined (Level 2)	ED-OIG/A11S0001 (FISMA Report) Issue 5: The Department's Security Training Program Needs Improvement (Repeat Finding)
Function 3: Detect - ISCM	Defined (Level 2)	Defined (Level 2)	ED-OIG/A11S0001 (FISMA Report) Issue 6: The Department's ISCM Program Needs Improvement (Repeat Finding)
Function 4: Respond - Incident Response	Defined (Level 2)	Defined (Level 2)	ED-OIG/A11S0001 (FISMA Report) Issue 7: The Department's Incident Response Program Needs Improvement (Repeat Finding)
Function 5: Recover - Contingency Planning	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	ED-OIG/A11S0001 (FISMA Report) Issue 8: The Department's and FSA's Contingency Planning Program Needs Improvement (Repeat Finding)
Overall	Not Effective	Not Effective	

Appendix D. Acronyms and Abbreviations

Department	U.S. Department of Education
DHS	Department of Homeland Security
EDUCATE	Education Department Utility for Communications, Applications, and Technology Environment
FISMA	Federal Information Security Modernization Act of 2014
FSA	Federal Student Aid
FY	fiscal year
ICAM	Identity, Credential, and Access Management
ISCM	Information Security Continuous Monitoring
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIVOT	Portfolio of Integrated Value-Oriented Technologies
SP	Special Publication
US-CERT	United States Computer Emergency Readiness Team

Department and FSA Management Comments



UNITED STATES DEPARTMENT OF EDUCATION

DATE: October 15, 2018

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

FROM: Mick Zais
Deputy Secretary
Department of Education

Mick Zais

James Manning
Acting Chief Operating Officer
Financial Student Aid

SUBJECT: Response to Discussion Draft Audit Report
The U.S. Department of Education's Federal Information Security Modernization Act of 2014 for Fiscal Year 2018
Control Number ED-OIG/A11S0001

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) 2018, Control Number ED-OIG/A11S0001. 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 (OCIO) recognizes that the objective of the OIG FISMA audit was to evaluate and determine the effectiveness of the Department's information security program policies, procedures, and practices. As the report indicates, the Department has taken numerous steps to strengthen the overall cybersecurity of its networks, systems, and data as highlighted by the improvement of the Recover Security Function from 'Defined' to 'Consistently Implemented.' Furthermore, the Department made progress in a number of metric scoring questions in the areas of Risk Management, Configuration Management, and Incident Response.

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 and Chief Operating Officer require that OCIO and FSA:

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

The Department of Education's mission is to promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access

OIG Recommendation 1.1: Incorporate additional measures to, at a minimum, achieve Level 4 Managed and Measurable status of the Risk Management program. (Repeat Recommendation).

Management Response: The Department concurs with this recommendation. The Department will continue to improve its Risk Management program and develop a corrective action plan by December 31, 2018 to address this recommendation.

OIG Recommendation 1.2: Ensure the completeness of individual corrective action plans for elements including remediation officials assigned, costs associated to remediate the weakness, and starting dates to remediate the weakness.

Management Response: The Department concurs with this recommendation. The Department will work with system stakeholders to ensure the completeness of individual corrective action plans for elements including remediation officials assigned, costs associated to remediate the weakness, and starting dates to remediate the weakness. The Department will develop a corrective action plan by December 31, 2018 to address the finding.

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 partially concurs with this recommendation. The Department has developed a number of processes to review Statements of Work (SOW) for proper contract language to include the OCIO Statement of Work review process and the FSA Information Resource Program Elements (IRPE) process. If the contracts included in the scope of the Inspector General's review occurred after the establishment of these processes, the Department will review the Statement of Work processes to ensure the contract clauses identified in the Inspector General's report are included. The Department does not intend to review contracts executed prior to the establishment of these processes. The Department will develop a corrective action plan by December 31, 2018 to address the finding.

REPORTING METRIC DOMAIN No.2: CONFIGURATION MANAGEMENT

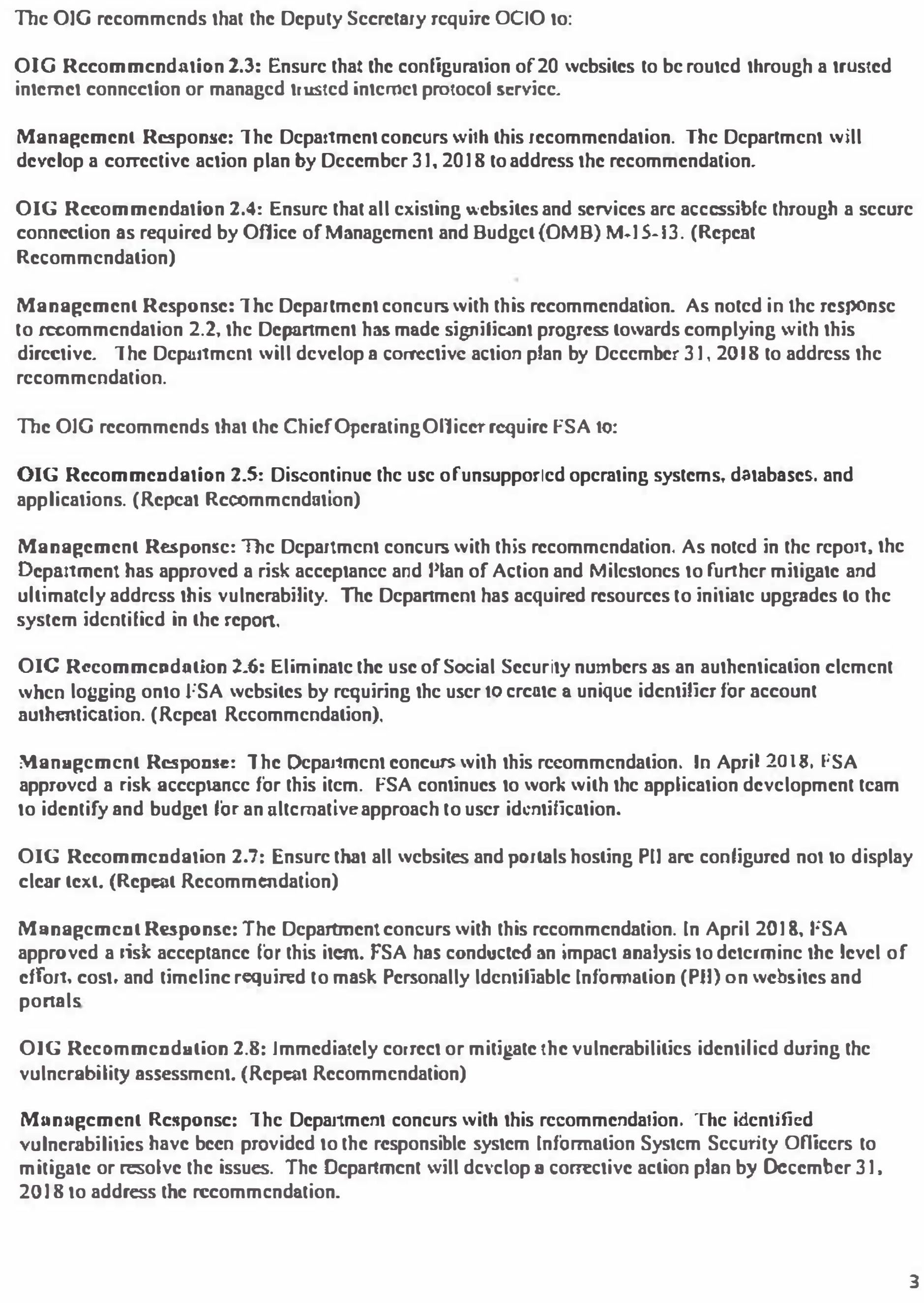
The OIG recommends that the Deputy Secretary and Chief Operating Officer require that OCIO and FSA:

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

Management Response: The Department concurs with this recommendation. The Department will develop a corrective action plan by December 31, 2018 to address the recommendation.

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

Management Response: The Department concurs with this recommendation. The Department has made significant progress in remediating this vulnerability including developing a master inventory of all Departmental websites. This inventory tracks website compliance to a number of cybersecurity requirements, for example, compliance with items outlined in the Department of Homeland Security Binding Operational Directive (BOD) 18-01. This inventory enables the Office of the Chief Information Officer to meet with business owners on a frequent basis to provide assistance and track the status of remediation activities. The Department will further efforts to mitigate this issue and develop a corrective action plan by December 31, 2018.



The OIG recommends that the Deputy Secretary require OCIO to:

OIG Recommendation 2.3: Ensure that the configuration of 20 websites to be routed through a trusted internet connection or managed trusted internet protocol service.

Management Response: The Department concurs with this recommendation. The Department will develop a corrective action plan by December 31, 2018 to address the recommendation.

OIG Recommendation 2.4: Ensure that all existing websites and services are accessible through a secure connection as required by Office of Management and Budget (OMB) M-15-13. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. As noted in the response to recommendation 2.2, the Department has made significant progress towards complying with this directive. The Department will develop a corrective action plan by December 31, 2018 to address the recommendation.

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

OIG Recommendation 2.5: Discontinue the use of unsupported operating systems, databases, and applications. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. As noted in the report, the Department has approved a risk acceptance and Plan of Action and Milestones to further mitigate and ultimately address this vulnerability. The Department has acquired resources to initiate upgrades to the system identified in the report.

OIG Recommendation 2.6: 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).

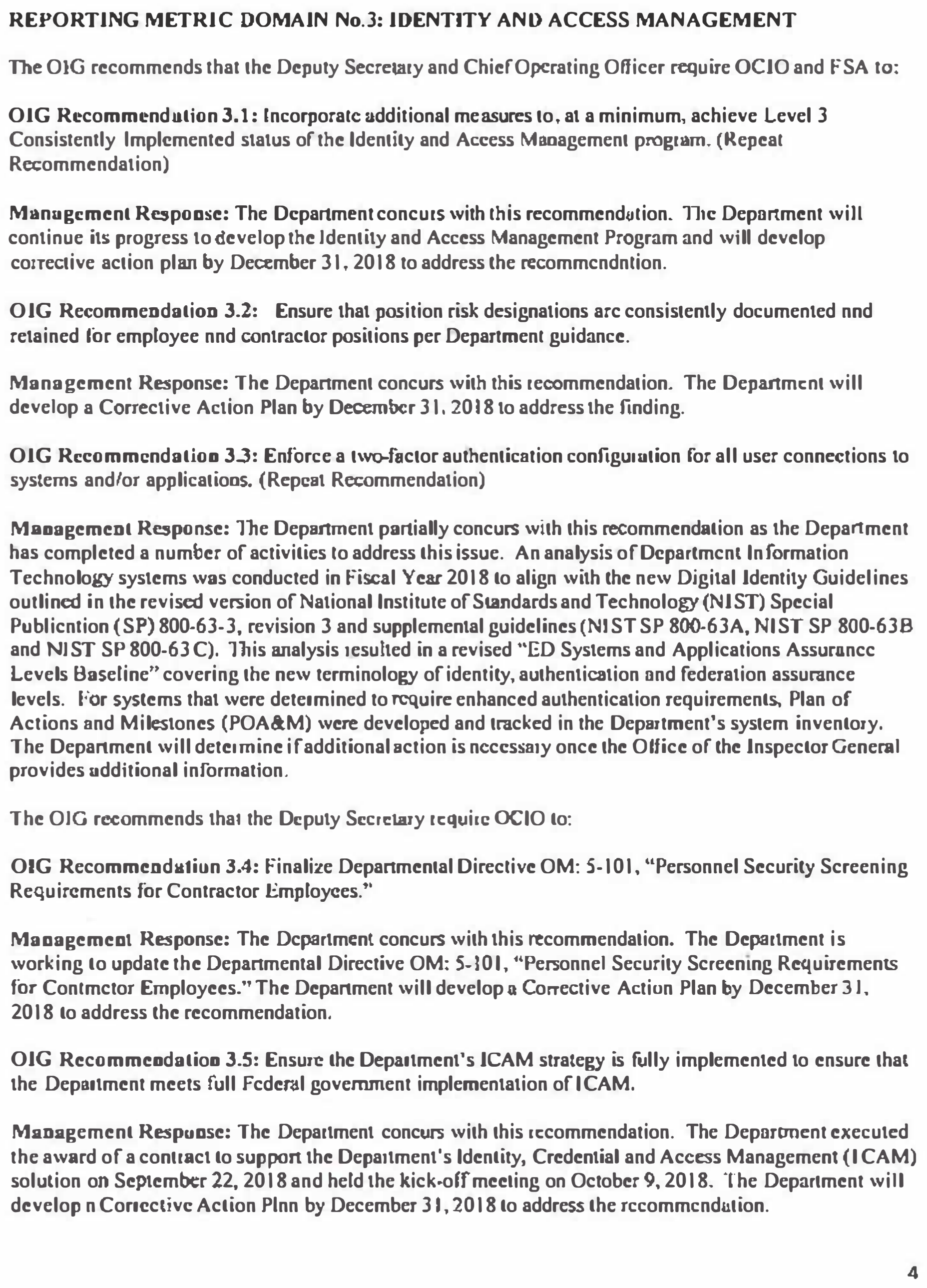
Management Response: The Department concurs with this recommendation. In April 2018, FSA approved a risk acceptance for this item. FSA continues to work with the application development team to identify and budget for an alternative approach to user identification.

OIG Recommendation 2.7: Ensure that all websites and portals hosting PII are configured not to display clear text. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. In April 2018, FSA approved a risk acceptance for this item. FSA has conducted an impact analysis to determine the level of effort, cost, and timeline required to mask Personally Identifiable Information (PII) on websites and portals

OIG Recommendation 2.8: Immediately correct or mitigate the vulnerabilities identified during the vulnerability assessment. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. The identified vulnerabilities have been provided to the responsible system Information System Security Officers to mitigate or resolve the issues. The Department will develop a corrective action plan by December 31, 2018 to address the recommendation.



REPORTING METRIC DOMAIN No.3: IDENTITY AND ACCESS MANAGEMENT

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

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

Management Response: The Department concurs with this recommendation. The Department will continue its progress to develop the Identity and Access Management Program and will develop corrective action plan by December 31, 2018 to address the recommendation.

OIG Recommendation 3.2: Ensure that position risk designations are consistently documented and retained for employee and contractor positions per Department guidance.

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 31, 2018 to address the finding.

OIG Recommendation 3.3: Enforce a two-factor authentication configuration for all user connections to systems and/or applications. (Repeat Recommendation)

Management Response: The Department partially concurs with this recommendation as the Department has completed a number of activities to address this issue. An analysis of Department Information Technology systems was conducted in Fiscal Year 2018 to align with the new Digital Identity Guidelines outlined in the revised version of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, revision 3 and supplemental guidelines (NIST SP 800-63A, NIST SP 800-63B and NIST SP 800-63C). This analysis resulted in a revised "ED Systems and Applications Assurance Levels Baseline" covering the new terminology of identity, authentication and federation assurance levels. For systems that were determined to require enhanced authentication requirements, Plan of Actions and Milestones (POA&M) were developed and tracked in the Department's system inventory. The Department will determine if additional action is necessary once the Office of the Inspector General provides additional information.

The OIG recommends that the Deputy Secretary require OCIO to:

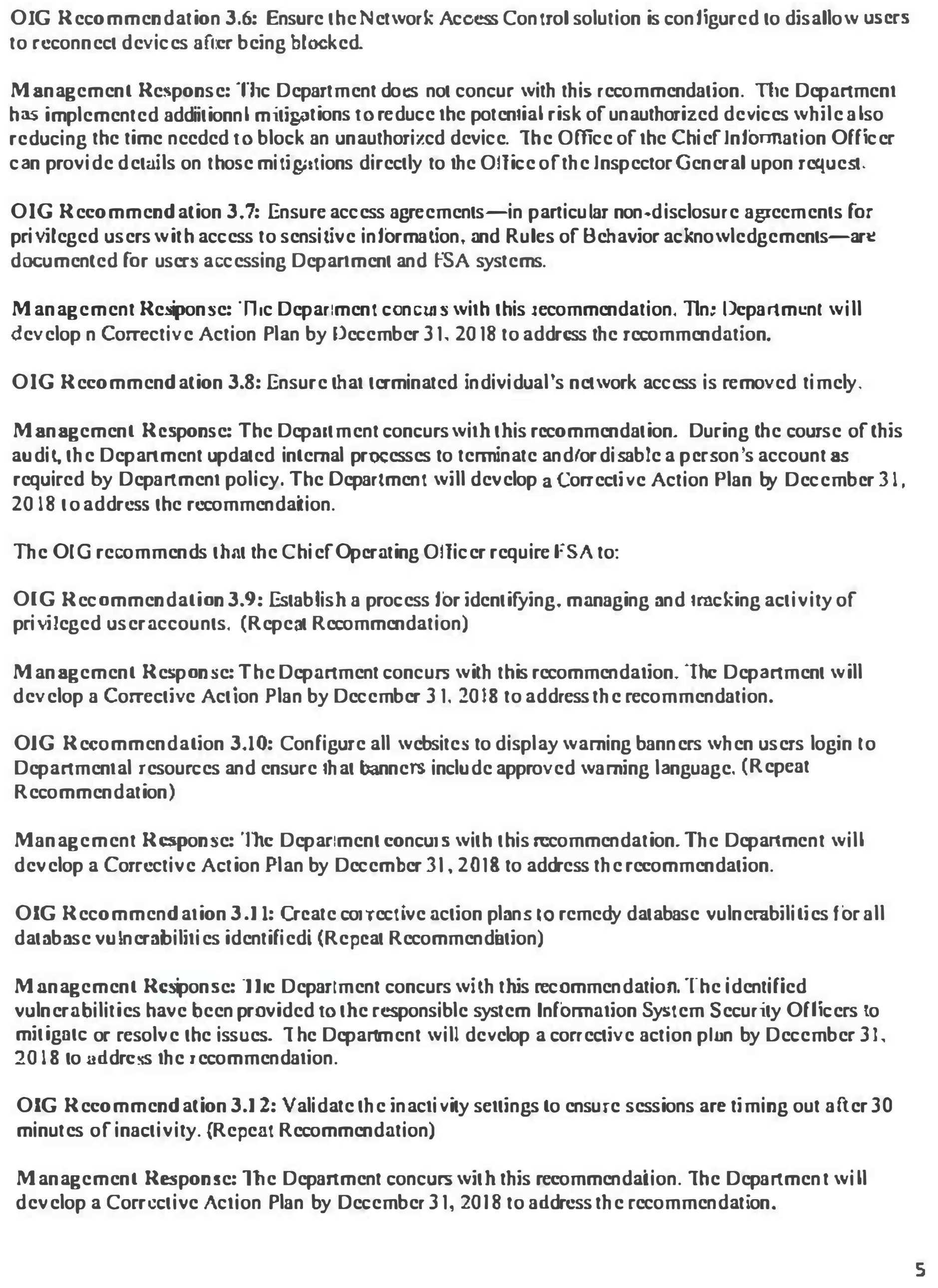
OIG Recommendation 3.4: Finalize Departmental Directive OM: 5-101, "Personnel Security Screening Requirements for Contractor Employees."

Management Response: The Department concurs with this recommendation. The Department is working to update the Departmental Directive OM: 5-101, "Personnel Security Screening Requirements for Contractor Employees." The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

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 executed the award of a contract to support the Department's Identity, Credential and Access Management (ICAM) solution on September 22, 2018 and held the kick-off meeting on October 9, 2018. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

4



OIG Recommendation 3.6: Ensure the Network Access Control solution is configured to disallow users to reconnect devices after being blocked.

Management Response: The Department does not concur with this recommendation. The Department has implemented additionnl mitigations to reduce the potential risk of unauthorized devices while also reducing the time needed to block an unauthorized device. The Office of the Chief Information Officer can provide details on those mitigations directly to the Office of the Inspector General upon request.

OIG Recommendation 3.7: Ensure access agreements—in particular non-disclosure agreements for privileged users with access to sensitive information, and Rules of Behavior acknowledgements—are documented for users accessing Department and FSA systems.

Management Response: The Department concurs with this recommendation. The Department will develop n Corrective Action Plan by December 31, 2018 to address the recommendation.

OIG Recommendation 3.8: Ensure that terminated individual's network access is removed timely.

Management Response: The Department concurs with this recommendation. During the course of this audit, the Department updated internal processes to terminate and/or disable a person's account as required by Department policy. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

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

OIG Recommendation 3.9: Establish a process for identifying, managing and tracking activity of privileged user accounts. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

OIG Recommendation 3.10: Configure all websites to display warning banners when users login to Departmental resources and ensure that banners include approved warning language. (Repeat Recommendation)

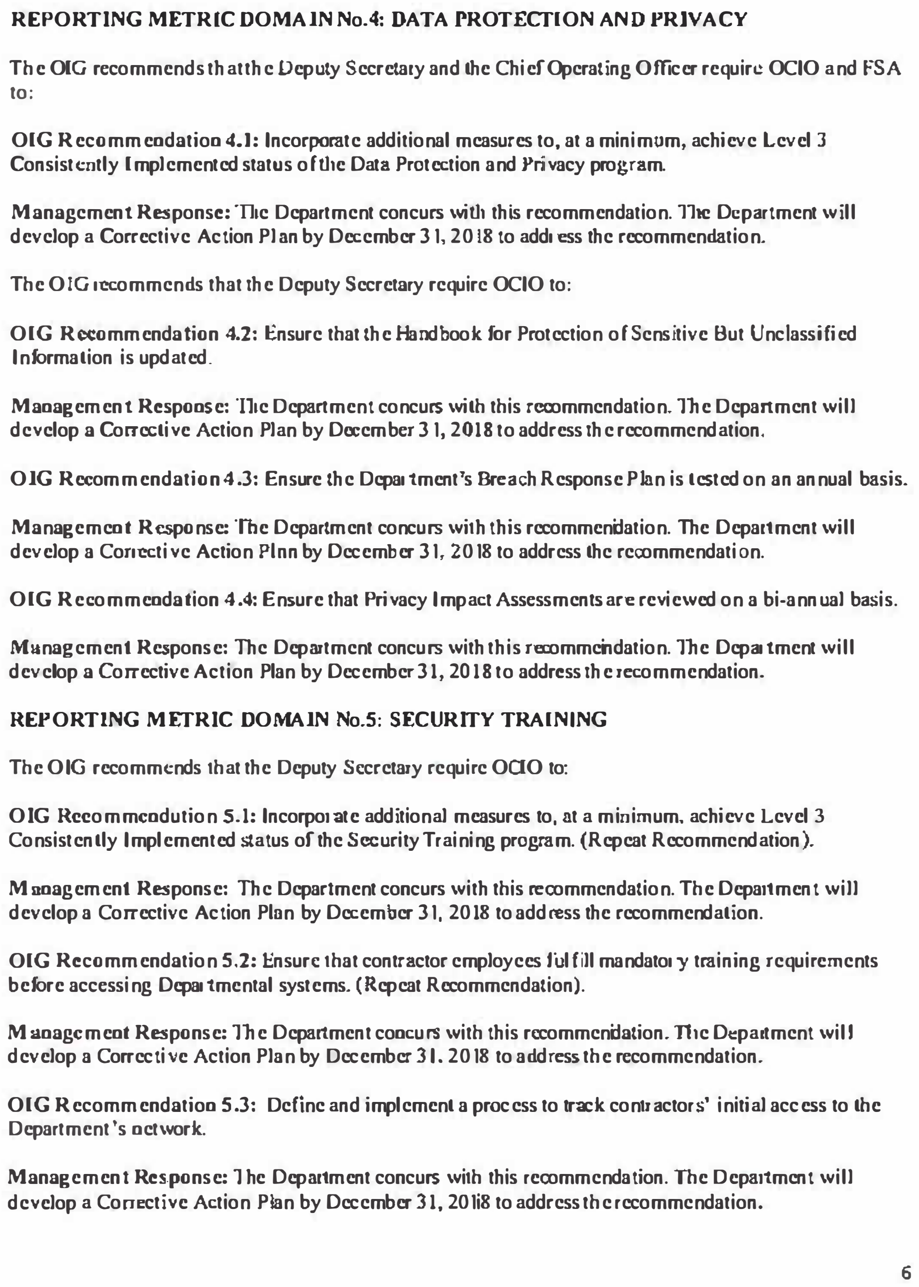
Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

OIG Recommendation 3.11: Create corrective action plans to remedy database vulnerabilities for all database vulnerabilities identifiedi (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. The identified vulnerabilities have been provided to the responsible system Information System Security Officers to mitigate or resolve the issues. The Department will develop a corrective action plan by December 31, 2018 to address the recommendation.

OIG Recommendation 3.12: Validate the inactivity settings to ensure sessions are timing out after 30 minutes of inactivity. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.



REPORTING METRIC DOMAIN No.4: DATA PROTECTION AND PRIVACY

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

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

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

The OIG recommends that the Deputy Secretary require OCIO to:

OIG Recommendation 4.2: Ensure that the Handbook for Protection of Sensitive But Unclassified Information is updated.

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

OIG Recommendation 4.3: Ensure the Department's Breach Response Plan is tested on an annual basis.

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

OIG Recommendation 4.4: Ensure that Privacy Impact Assessments are reviewed on a bi-annual basis.

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

REPORTING METRIC DOMAIN No.5: SECURITY TRAINING

The OIG recommends that the Deputy Secretary require OCIO to:

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

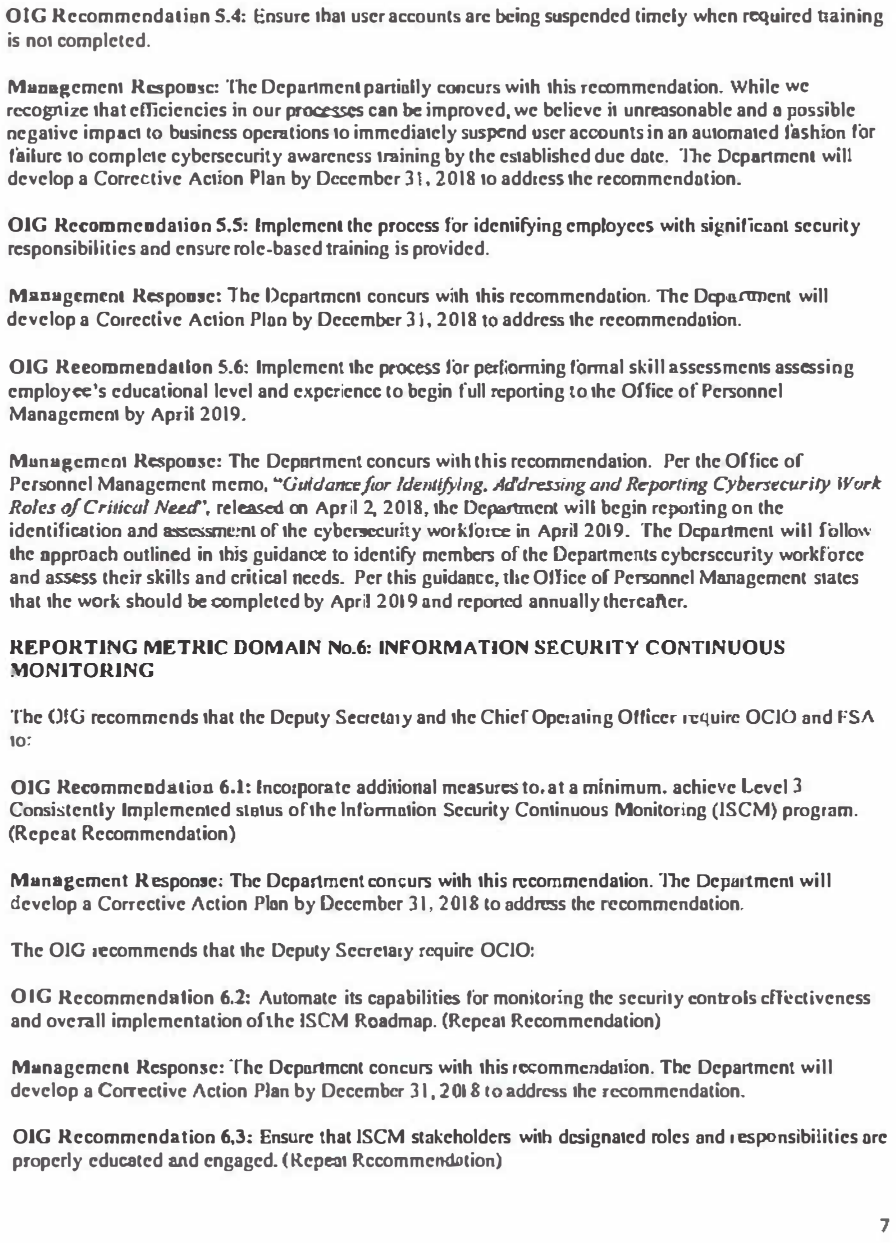
Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

OIG Recommendation 5.2: Ensure that contractor employees fulfill mandatory training requirements before accessing Departmental systems. (Repeat Recommendation).

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

OIG Recommendation 5.3: Define and implement a process to track contractors' initial access to the Department's network.

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.



OIG Recommendation 5.4: Ensure that user accounts are being suspended timely when required training is not completed.

Management Response: The Department partially concurs with this recommendation. While we recognize that efficiencies in our processes can be improved, we believe it unreasonable and a possible negative impact to business operations to immediately suspend user accounts in an automated fashion for failure to complete cybersecurity awareness training by the established due date. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

OIG Recommendation 5.5: Implement the process for identifying employees with significant security responsibilities and ensure role-based training is provided.

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

OIG Recommendation 5.6: Implement the process for performing formal skill assessments assessing employee's educational level and experience to begin full reporting to the Office of Personnel Management by April 2019.

Management Response: The Department concurs with this recommendation. Per the Office of Personnel Management memo, "*Guidance for Identifying, Addressing and Reporting Cybersecurity Work Roles of Critical Need*", released on April 2, 2018, the Department will begin reporting on the identification and assessment of the cybersecurity workforce in April 2019. The Department will follow the approach outlined in this guidance to identify members of the Departments cybersecurity workforce and assess their skills and critical needs. Per this guidance, the Office of Personnel Management states that the work should be completed by April 2019 and reported annually thereafter.

REPORTING METRIC DOMAIN No.6: INFORMATION SECURITY CONTINUOUS MONITORING

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

OIG Recommendation 6.1: Incorporate additional measures to, at a minimum, achieve Level 3 Consistently Implemented status of the Information Security Continuous Monitoring (ISCM) program. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

The OIG recommends that the Deputy Secretary require OCIO:

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

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

OIG Recommendation 6.3: Ensure that ISCM stakeholders with designated roles and responsibilities are properly educated and engaged. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

OIG Recommendation 6.4: Ensure all Information Authorizing Officials, Information System Owners, and Information System Security Officers establish and utilize accounts within the Cyber Security Assessment and Management tool, and that required points of contacts are identified. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

OIG Recommendation 6.5: Ensure the completion of Phases 1 and 2 of the Continuous Diagnostics Mitigation (CDM) program. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. Although the Department has made progress in respect to this recommendation as provided in evidence submitted for the fiscal year 2017 corrective action, the Department will develop a Corrective Action Plan by December 31, 2018 outlining additional steps to address the recommendation.

REPORTING METRIC DOMAIN No.7: INCIDENT RESPONSE

The OIG recommends that the Deputy Secretary require OCIO to:

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

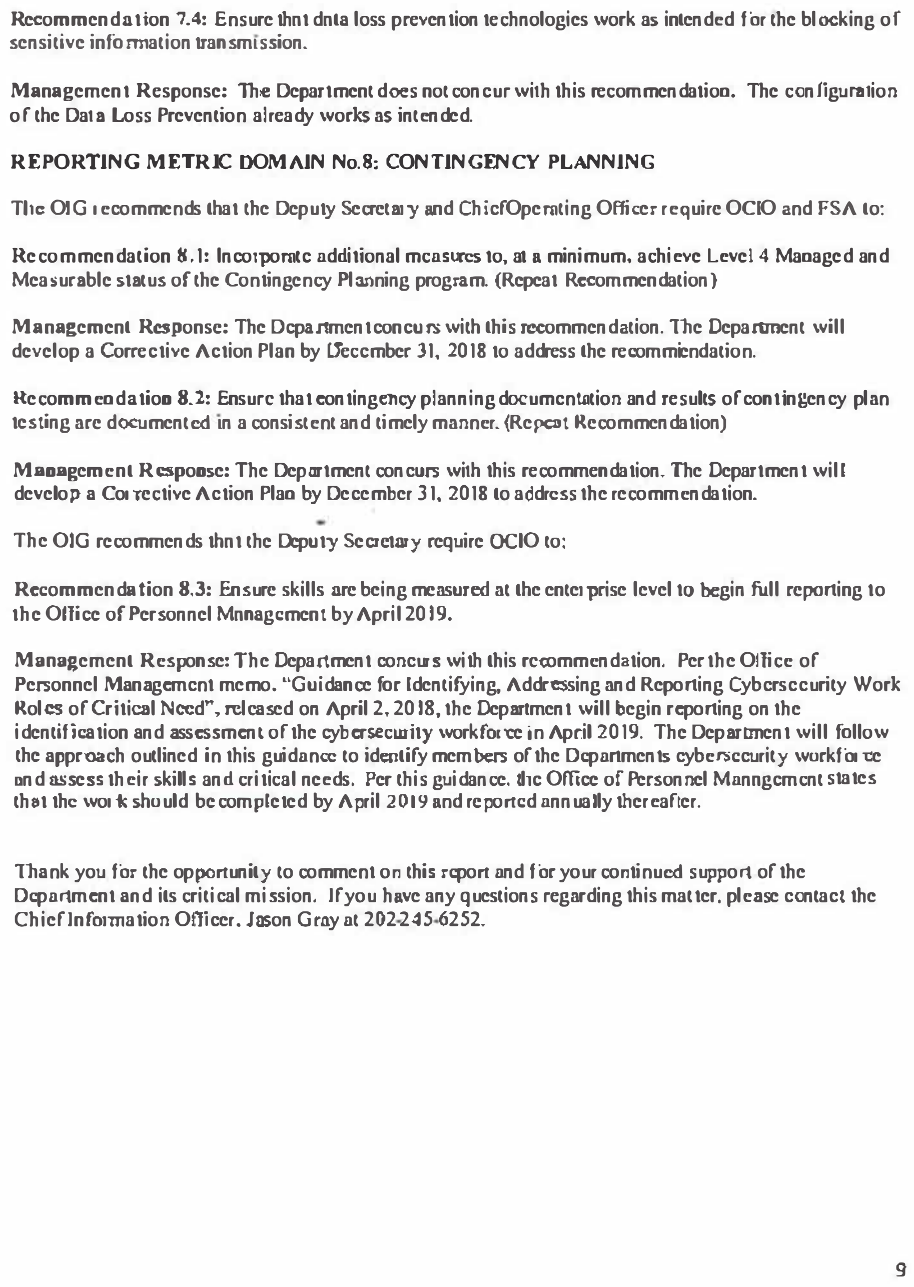
Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

Recommendation 7.2: Ensure that incidents are consistently submitted to the United States Computer Emergency Readiness Team (US-CERT) and OIG within the required timeframe and all incidents are consistently categorized. (Repeat Recommendation)

Management Response: The Department partially concurs with this recommendation. The Department agrees that there are efficiencies to be gained in incident management processes. However, the Department would like to point out that approximately 2% of all incident tickets were reported as incorrectly categorized. The Department has reported tickets based on current reporting guidance listed in the Federal Incident Notification Guidance (FING). Tickets for similar alerts (example; McAfee ePO) may be categorized as a Category 1, Category 2, or Category 3 depending on the severity of the event. The differences in categorization for such alerts are not due to inconsistency, but instead because the events involved a different set of circumstances, as such the Department believes it is unrealistic to achieve 100% accuracy at any point in time. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

Recommendation 7.3: Enable incident response tools/technologies to function on an enterprise basis.

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.



Recommendation 7.4: Ensure that data loss prevention technologies work as intended for the blocking of sensitive information transmission.

Management Response: The Department does not concur with this recommendation. The configuration of the Data Loss Prevention already works as intended.

REPORTING METRIC DOMAIN No.8: CONTINGENCY PLANNING

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

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

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

Recommendation 8.2: Ensure that contingency planning documentation and results of contingency plan testing are documented in a consistent and timely manner. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. The Department will develop a Corrective Action Plan by December 31, 2018 to address the recommendation.

The OIG recommends that the Deputy Secretary require OCIO to:

Recommendation 8.3: Ensure skills are being measured at the enterprise level to begin full reporting to the Office of Personnel Management by April 2019.

Management Response: The Department concurs with this recommendation. Per the Office of Personnel Management memo. "Guidance for Identifying, Addressing and Reporting Cybersecurity Work Roles of Critical Need", released on April 2, 2018, the Department will begin reporting on the identification and assessment of the cybersecurity workforce in April 2019. The Department will follow the approach outlined in this guidance to identify members of the Departments cybersecurity workforce and assess their skills and critical needs. Per this guidance, the Office of Personnel Management states that the work should be completed by April 2019 and reported annually thereafter.

Thank you for the opportunity to comment on this report and for your continued support of the Department and its critical mission. If you have any questions regarding this matter, please contact the Chief Information Officer, Jason Gray at 202-245-6252.

cc: Jason Gray, Chief Information Officer, Office of the Chief Information Officer

Ann Kim, Deputy Chief Information Officer, Office of the Chief Information Officer

John Fare, Acting Chief Information Officer, Federal Student Aid

Wanda Broadus, Acting Deputy Chief Information Officer, Federal Student Aid

Steven Hernandez, Director, Information Assurance Services, Office of the Chief Information Officer

Dan Commons, Director, Information Technology Risk Management Group, Federal Student Aid

Kelly Cline, Audit Liaison, Office of the Chief Information Officer

Stefanie Clay, Audit Liaison, Federal Student Aid

Bucky Methfessel, Senior Counsel for Information & Technology, Office of the General Counsel

Kala Surprenant, Senior Counsel for Oversight, Office of the General Counsel

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

10