The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report For Fiscal Year 2016

FINAL AUDIT REPORT

ED-OIG/A11Q0001
November 2016

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

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

NOTICE

Statements that managerial practices need improvements, as well as other conclusions and recommendations in this report, represent the opinions of the Office of Inspector General. Determinations of corrective action to be taken will be made by the appropriate Department of Education officials.

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

Abbreviations and Acronyms Used in this Report

ACS	Administrative Communications Systems
CAMS	Case and Activity Management System
COD	Common Origination and Disbursement
Dell	Dell Services Federal Government
Department	U.S. Department of Education
EDCAPS	Education Central Automated Processing System
EDSTAR	Education Security Tracking and Reporting System
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
ISCM	Information Security Continuous Monitoring
IT	Information Technology
Metric Domain	Fiscal Year 2016 Federal Information Security Modernization Act of 2014 Metric Domains
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
PAS	Person Authentication Service
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
Security Functions	Cybersecurity Framework Security Functions
SP	Special Publication
SSLv3	Secure Socket Layer, Version 3
TLS	Transport Layer Security

UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

November 10, 2016

Memorandum

TO: James Cole, Jr.
General Counsel, Delegated the Duties of Deputy Secretary
Office of the Deputy Secretary

Ted Mitchell
Under Secretary
Office of the Under Secretary

FROM: Charles E. Coe, Jr.
Assistant Inspector General
Information Technology Audits and Computer Crime Investigations
Office of Inspector General

SUBJECT: Final Audit Report
The U.S. Department of Education's Federal Information Security Modernization Act of 2014 for Fiscal Year 2016
Control Number ED-OIG/A11Q0001

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 2016. An electronic copy has been provided to your Audit Liaison Officers. We received your comments on the findings and recommendations in our draft report.

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

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

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

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

Enclosure

Cc:

Jason Gray, Chief Information Officer, Office of the Chief Information Officer
Keith Wilson, Chief Information Officer, Federal Student Aid
Kenneth Moore, Deputy Chief Information Officer, Office of the Chief Information Officer
Leslie Willoughby, Deputy Chief Information Officer, Federal Student Aid
Daniel Galik, Director, Information Assurance Services, Office of the Chief Information Officer
Linda Wilbanks, PhD, Director, Information Technology Risk Management Group, Federal Student Aid
Jim Harrell, 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

Page

EXECUTIVE SUMMARY

This report constitutes the Office of Inspector General's independent evaluation of the U.S. Department of Education's (Department) information technology security program and practices, as required by the Federal Information Security Modernization Act of 2014 (FISMA). Our report is based on, and incorporates, the Fiscal Year (FY) 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics V1.1.3 (September 26, 2016) (FY 2016 FISMA Metrics) prepared by the Office of Management and Budget, the U.S. Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency, in consultation with the Federal Chief Information Officer Council.

What Was Our Objective?

Our objective was to determine whether the Department's and Federal Student Aid's (FSA) overall information technology security programs and practices were generally effective as they relate to Federal information security requirements. The FY 2016 FISMA Metrics are grouped into eight "metric domains" and organized around the five Cybersecurity Framework Security Functions (security functions) outlined in the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity. The five security functions and their associated FY 2016 FISMA Metric Domains (metric domains) are structured as follows:

- Identify security function includes two metric domains—Risk Management and Contractor Systems,
- Protect security function includes three metric domains—Configuration Management, Identity and Access Management, and Security and Privacy Training,
- Detect security function includes one metric domain—Information Security Continuous Monitoring,
- Respond security function, includes one metric domain—Incident Response, and
- Recover security function, includes one metric domain—Contingency Planning.[1]

In the FY 2015 FISMA audit, we measured effectiveness by each metric domain. However, for FY 2016, Inspectors General are being asked to assess the effectiveness of the each security function using a maturity level scoring distribution. The scoring distribution is based on five maturity levels outlined in the FY 2016 FISMA metrics: (1) Ad-hoc, (2) Defined, (3) Consistently Implemented, (4) Managed and Measurable, and (5) Optimized. Level 1, Ad-hoc, is the lowest maturity level and Level 5, Optimized, is the highest maturity level. For a security function to be considered effective, agencies' security programs must score at or above Level 4, Managed and Measurable.

[1] For the areas of Information Security Continuous Monitoring and Incident Response, the Office of Inspector General was required to assess the maturity level of each area based on a maturity model. For the remaining areas, the Office of Management and Budget and the U.S. Department of Homeland Security developed "maturity indicators;" for FY 2017, the Council of the Inspectors General on Integrity and Efficiency (together with the Office of Management and Budget and the U.S. Department of Homeland Security) plans to develop maturity models for the remaining areas.

To meet the 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 with respect to meeting the security requirements for the information system in its operational environment.[2]

What We Reviewed

Within each metric domain, we reviewed information technology controls, policies and procedures, and current processes to determine whether they operated as intended as specified by the FY 2016 FISMA Metrics. We report our results on each of these metric domains, as required, in Enclosure 1.

Based on our work on these metric domains, along with additional work we did to test the Department's and FSA's program effectiveness in each domain, we scored effectiveness on the maturity level reached within each of the five security functions. For Continuous Monitoring Management and Incident Response, we used maturity models to score the maturity levels reached for the Detect and Respond security functions, respectively.

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 assessment and penetration testing of Web applications and application infrastructure; (3) follow-up vulnerability assessment and testing of the Common Origination and Disbursement system components infrastructure; (4) verification of training evidence; (5) testing of remote access control settings; and (6) observation of Education Department Utility for Communications, Applications, and Technology Environment's disaster recovery exercise. In addition, we met with Office of the Chief Information Officer's Policy and Planning team to discuss their roles and responsibilities and dissemination of departmental policies. We summarize results of our discussions with the Department in the "Other Matters" section of this report.

During the FY 2015 FISMA audit, we found that the Department was not generally effective in four metric domains—Information Security Continuous Monitoring, Configuration Management, Incident Response and Reporting, and Remote Access Management. While we determined that the Department's and FSA's information technology security programs were generally effective in key aspects of three metric domains, we also report that improvements are needed.

What We Found

To measure the effectiveness of an information technology security program and determine the maturity level for each of the security functions, a scoring system based on the maturity levels mentioned above. For each maturity level achieved, a scoring distribution is determined that, when added for all the security functions, will provide an overall score and a conclusion on the effectiveness of an agency's information security program. An agency can obtain a maximum

[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.

score of 20 points for each security function and overall score of 100 points in total. To be considered effective, an agency must score at least 18 in any individual Security Function or 80 points or above in aggregate.[3]

We scored the Department and FSA's information technology security programs to be 53 points out of 100. Based on this score, the Department and FSA's overall information security programs are deemed generally not effective. Specifically, we found although the Department and FSA were generally effective in two of the five Security Functions—Identify and Recover, they were not generally effective in three security functions—Protect, Detect, and Respond.

The following table provides a synopsis on how the Department and FSA scored overall in each of the security functions.

Security Functions	Metric Domains	Score
Identify	Risk Management and Contractor Systems	20/20
Protect	Configuration Management, Identity and Access Management, and Security and Privacy Training	7/20
Detect	Information Security Continuous Monitoring	3/20
Respond	Incident Response	3/20
Recover	Contingency Planning	20/20
Effective: Yes / [✓ No]	**Total**	**53/100**

Note: Each function is worth a maximum of 20 points. For the Fiscal Year 2016 Inspector General metrics, an agency must score 80 or higher to be considered to have an effective information technology security program.

Within the eight metric domains, we identified findings in five areas: (1) Configuration Management (2) Identity and Access management; (3) Security and Privacy Training; (4) Information Security Continuous Monitoring; and (5) Incident Response.

We found the Department and FSA had made improvements with their respective risk management programs with the continuous growth in the establishment of a risk management framework. In particular, both have moved from the 3-year system authorization process to a real-time, continuous program for both contractor and agency systems' authorizations to operate. For contractor systems, we found that the Department established and implemented a process to ensure that contracts, statements of work, and solicitations for systems and services include appropriate information security and privacy requirements. For contingency planning programs, we found that the Department and FSA are developing and successfully testing contingency plans annually at disaster recovery sites.

[3] Because this is the first year for the new scoring method, the Office of Management and Budget decided that an aggregate of 80 points or above will be considered as being effective instead of the 90 points that the scoring would normally have required.

Although the Department and FSA made progress in strengthening their information security programs, weaknesses remained and the Department and FSA's information systems continued to be vulnerable to security threats. For configuration management, we found (1) select policies and procedures are not current with National Institute of Standards and Technology and Departmental guidance, (2) appropriate application connection protocols were not being used, and (3) the Department is unable to prevent unauthorized devices from being connected to the network. All three of those findings identified were also findings we identified during our FY 2015 FISMA audit and still continue to exist. In addition, for configuration management, through our vulnerability assessment testing, we found that the Department's and FSA's controls over Web applications, as well as the application's network infrastructure need improvement. Specifically, we found that the implementation and management of the technical security architecture supporting the Department's and FSA's applications requires strengthening to more effectively restrict unauthorized access to information resources. More importantly, the Office of the Chief Information Officer and FSA did not implement remedial actions for previously identified security weaknesses and did not establish a proactive enterprise-wide process to fix similar vulnerabilities identified during previous audits.

For identity access management, we performed database management assessments that identified vulnerabilities, configuration errors, rogue installations, and access issues for databases residing in the Contracts & Acquisitions Management System, Education Security Tracking and Reporting, the Person Authentication Service, and the Common Origination and Disbursement environments that manage sensitive and private data that impact both students within FSA and the Department. Further, we found that two-factor authentication for non-privileged users is not effectively implemented and external network connections did not use two-factor authentication—another repeat finding from the FY 2015 FISMA audit. We also found that although the Department established processes and controls to ensure an effective security and privacy training program, the Department can improve its assessment of individuals with significant security and privacy responsibilities.

For this year's reporting, we are reporting two of the metric domains under a maturity model—Information Security Continuous Monitoring (ISCM) and Incident Response. Since our FY 2015 FISMA reporting, we found that the Department has improved its ISCM program; for example, it developed comprehensive policies and procedures for security assessments and performed ongoing security authorizations. However, the Department and FSA still remain at Maturity Level 1—Ad-hoc. Although the Department and FSA defined how they would implement their ISCM activities, their ISCM processes, performance measures, policies, and procedures have not been implemented consistently across the organization. For incident response, the Department and FSA have not fully developed, implemented, or enforced policies and procedures to manage an effective incident response program and are therefore at Maturity Level 1—Ad-hoc. Specifically, the Department did not have procedures to assess skills, knowledge, and resources; therefore, it could not implement or enforce those procedures.

Our answers to the questions in the Department of Homeland Security metrics template, which will become the CyberScope report, are shown in Enclosure 1.

What We Recommend

This report contains 11 findings, 5 of which are repeat findings previous FISMA audit reports. We make 15 recommendations (6 of which are repeat recommendations) to assist the Department and FSA with increasing the effectiveness of their information security program so that they fully comply with all applicable requirements of FISMA, the Office of Management and Budget, the Department of Homeland Security, and the National Institute of Standards and Technology. During our FY 2015 FISMA audit, we made 26 recommendations to the Department and FSA to address the 16 findings that we identified. As of October 2016, the Department and FSA reported that they have completed corrective actions for 25 of the 26 recommendations. However, despite completing corrective actions, we continue to identify repeat findings and recommendations in both the Configuration Management and Identity and Access Management metric domains. Although the Department and FSA may have taken action on specific findings, systemic issues persist in these metric domains on an enterprise-level.

The Department concurred with 14 of the 15 recommendations and partially concurred with recommendation 4.4. We summarized and responded to specific comments in the "Audit Results" section of this report. We considered the Department's comments, but did not revise our findings or recommendations. Further, the Department's response suggests that the degree of changes to the FY 2016 FISMA metrics, specifically, the revised scoring methodology, did not capture the improvements and progress made by the Department in FY 2016. We agree with the Department, as discussed during our exit conference, that the scoring methodology was updated in September 2016 from its original release in June 2016. However, changes to the scoring methodology did not impact the FISMA metrics or the security controls being evaluated to determine the effectiveness of the Department's information security program. The Department was made aware of the FY 2016 FISMA metrics when they were released by OMB in June 2016. While the scoring methodology was changed in September 2016, the underlying metrics remained unchanged after their release in June, so any improvements made by the Department during our audit would be reflected in how we applied the metrics.

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 was responsible for creating and overseeing policies, standards, and guidelines for information security and has the authority to approve agencies' information security programs. OMB was 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, the Federal Information Security Modernization Act of 2014 (FISMA), Public Law 113-283, was enacted to update the Federal Information Security Management Act of 2002 by (1) reestablishing the oversight authority of the Director of OMB with respect to agency information security policies and practices and (2) setting forth authority for the Department of Homeland Security Secretary to administer the implementation of such policies and practices for information systems.

In addition, FISMA revised the Federal Information Security Management Act of 2002 requirement for Offices of Inspectors General (OIG) to annually assess agency "compliance" with information security policies, procedures, standards, and guidelines to now assess the "effectiveness" of the agency's information security program. It also codified certain information security requirements related to continuous monitoring that OMB previously established. FISMA specifically mandates that each evaluation under this section must include (1) testing of the effectiveness of information, security policies, procedures, and practices of a representative subset of the agency's information systems and (2) an assessment of the effectiveness of the information security policies, procedures, and practices of the agency.

OMB, the Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency developed the Fiscal Year (FY) 2016 Inspector General FISMA Reporting Metrics V1.1.3 (September 26, 2016) (FY 2016 FISMA Metrics) in consultation with the Federal Chief Information Officer Council. The FY 2016 FISMA Metrics organized around the five information Cybersecurity Framework Security Functions (security functions) outlined in the National Institute of Standards and Technology's "Framework for Improving Critical Infrastructure Cybersecurity": (1) Identify, (2) Protect, (3) Detect, (4) Respond, and (5) Recover.[4] This framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides Inspectors General with guidance for assessing the maturity of controls to address those risks, as highlighted in Table 1.

Table 1. Aligning the Security Functions to the Fiscal Year 2016 Inspector General FISMA Metric Domains

Security Functions	Fiscal Year 2016 Inspector General Metric Domains
Identify	Risk Management and Contractor Systems
Protect	Configuration Management, Identity and Access Management, and Security and Privacy Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

[4] 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.

For FY 2015, the Council of the Inspectors General on Integrity and Efficiency, in coordination with the Department of Homeland Security, OMB, NIST, and other key stakeholders, established the maturity model for information security continuous monitoring (ISCM). The maturity model is designed to provide perspective on the overall status of information security within an agency, as well as across agencies. In FY 2016, this effort continued by establishing an Incident Response maturity model, and plans to extend the maturity model to other security functions for OIGs to use in their FY 2017 FISMA reviews.

For the five Security Functions, OIGs were required to assess the agency's maturity level. The maturity level of the Security Function is based on the scoring identified in Table 2.

Table 2. Level of Maturity and Scoring Description

Maturity Level	Scoring Description
Level 1: Ad-hoc	Agencies automatically receive points regardless of their achievements in this maturity level.
Level 2: Defined	For the *Identify, Protect, and Recover* function areas, has met half or greater of all metrics designated in the "Defined" level. For the *Detect and Respond* function areas, has met all metrics designated in the "Ad-hoc" level and half or greater of the metrics designated in the "Defined" level.
Level 3: Consistently Implemented	For all function areas, met all metrics designated at the "Defined" level and half or greater of the metrics designated in the "Consistently Implemented" level.
Level 4: Managed and Measureable	For all function areas, met all metrics designated in the "Consistently Implemented" level and half or greater of the metrics designated in the "Managed and Measurable" level.
Level 5: Optimized	For all functional areas, met in all metrics designated in the "Management and Measureable" and "Optimized" levels.

For both the Detect and Respond security functions, the agency's maturity level is measured by the maturity level reached within the maturity model. For the Identify, Protect, and Recover security functions, the U.S. Department of Education's (Department) maturity level is determined on how many metrics they were able to cumulatively achieve by meeting the intent of the metric questions. The final score for an agency's information security program is the total of all five security functions. An agency's information security program is considered effective if the final score is 80 or greater.

Agencies with security functions that score at or above the Managed and Measurable (Levels 4 or 5) have "effective" programs in accordance with the effectiveness definition in NIST Special Publication (SP) 800-53, Revision 4, "Security and Privacy for Federal Information Systems and Organizations."

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

Departmental Systems and Security Program Description

In September 2007, the Department entered into a contract with Dell Services Federal Government (Dell) to provide and manage information technology (IT) infrastructure services to the Department under the Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) system. The contract established a contractor-owned and contractor-operated IT service model for the Department under which Dell provides the enterprise IT platform and network infrastructure to support Department employees in meeting the Department's mission. The contract was awarded as a 10-year, performance-based, indefinite-delivery, indefinite-quantity contract with fixed unit prices but was due to expire in November 2017. Under this contract, Dell owns all of the IT hardware and operating systems, including wide-area and local-area network devices, network servers, routers, switches, external firewalls, voice mail, and the Department's laptops and workstations. Dell also provides help desk services and all personal computer services. Dell also manages the Department's Virtual Data Center,[5] which is located at the contractor's facility in Plano, Texas. The Virtual Data Center is a general support system into which Federal Student Aid (FSA) consolidated many of its student financial aid program systems to improve interoperability and reduce costs. It serves as the hosting facility for FSA systems that process student financial aid applications, provide schools and lenders with eligibility determinations, and support payments from and repayment to lenders. It consists of a network infrastructure, servers, and the corresponding operating systems. Many of the financial aid applications that are hosted at Virtual Data Center are operated by other contractors. The Department's total spending for IT investments for FY 2016 was $689 million.

One of FSA's systems, Common Origination and Disbursement (COD) system, was previously hosted at both the Virtual Data Center and Total Systems Services, Inc., data centers. As of 2016, it will be hosted, exclusively at the Total Systems Services data center in Columbus, Georgia, which is operated through its prime contractor Accenture. The COD system is a technical solution and streamlined method for processing, storing, and reconciling Pell Grant and Direct Loan financial aid data. More specifically, the COD system simplifies the process for schools to obtain financial aid for their students.

Primarily through the Office of the Chief Information Officer (OCIO), the Department monitors and evaluates the contractor-provided IT services through a service-level agreement framework. OCIO advises and assists the Secretary and other senior officials to ensure that the Department acquires and manages IT resources in a manner that is consistent with the requirements of the Clinger-Cohen Act of 1996,[6] FISMA, and OMB Memorandum A-130.[7] OCIO is responsible for

[5] The Dell contract for the Virtual Data Center operations was up for re-compete in May 2015. On September 25, 2015, Hewlett Packard Enterprise Services was awarded the contract for the Virtual Data Center.

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

implementing the operative principles established by legislation and regulation, establishing a management framework to improve the planning and control of IT investments, and leading change to improve the efficiency and effectiveness of the Department's operations.

Fiscal Year 2015 FISMA Audit Results

During last year's FISMA audit, we identified 16 findings and provided 26 recommendations that would address the conditions noted in the report. The Department concurred with 23 recommendations, partially concurred with 3, and provided corrective action plans on how it would address the recommendations. In general, our findings identified:

- undefined or inconsistent continuous monitoring activities,
- outdated policies and procedures,
- the use of unsecure application protocols,
- outdated digital certificates for Web sites,
- the lack of implementation of a network access control solution,
- access controls issues for systems, and
- weak incident detection and prevention controls.

The Department and FSA agreed to corrective actions such as updating policies and procedures, establishing new procedures, conducting internal testing on remote connection controls, updating security documentation as needed, and where appropriate, instituting secure connection protocols for its systems. As of October 2016, the Department and FSA reported that they had completed corrective actions for 25 of the 26 recommendations.

AUDIT RESULTS

Based on the requirements specified in FISMA and the FY 2016 FISMA Metrics instructions, our audit focused on reviewing the five security functions and associated metric domains: Identify (Risk Management and Contractor Systems), Protect (Configuration Management, Identity and Access Management, and Security and Privacy Training), Detect (Information Security Continuous Monitoring), Respond (Incident Response), and Recover (Contingency Planning).[8]

We scored the Department's and FSA's IT security programs to be 53 points out of 100. Based on this score, the Department and FSA's overall IT security programs and practices were not generally effective as they relate to Federal information security requirements. Specifically, we found that although the Department and FSA were general effective in two of the five security functions (Identify and Recover), they were not generally effective in three security functions (Protect, Detect, and Respond). See the table in the Executive Summary for a synopsis of how the Department and FSA scored in each of security functions.

We identified findings in Configuration Management, Identity and Access Management, Security and Privacy Training, ISCM, and Incident Response metric domains. Our findings in these metric domains included repeat findings from the following OIG reports issued from FYs 2011 through 2015:

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

[8] For the metric domains, ISCM and incident response, the OIG General was required to assess the maturity level of each area based on a maturity model. For the remaining areas, the OMB and the U.S. Department of Homeland Security developed "maturity indicators"; for fiscal year 2017, the Council of the Inspectors General on Integrity and Efficiency (together with the OMB and the U.S. Department of Homeland Security) plans to develop maturity models for the remaining areas.

SECURITY FUNCTION 1—IDENTIFY

Based on the maturity model indicator scoring, we determined that the Department and FSA's "Identify" security function scored 20 points and is at Level 5: Optimized, which is categorized as being effective. Specifically, the Department and FSA developed a comprehensive governance structure and organization-wide risk management strategy and program that included comprehensive agency policies and procedures consistent with OMB policy and applicable NIST guidelines. In addition, the Department and FSA have instituted security authorization programs; established a Cybersecurity Risk Management Framework; maintained an active system inventory; established policy and a process for remediating and tracking security risks; established a risk scoring methodology; established a program to oversee systems operated on its behalf by contractors or other entities defined by comprehensive agency policies and procedures that address OMB policy and applicable NIST guidelines; and established and implemented a process to ensure that contracts, statements of work, and solicitations for systems and services include appropriate information security and privacy requirements.

The Identify security function comprises the Risk Management and Contractor Systems metric domains. In prior years' reporting, the Plan of Action and Milestones (POA&M) area was reported as a separate metric domain. However, for FY 2016 FISMA reporting, POA&M metric questions are incorporated into the Risk Management metric domain.

METRIC DOMAIN 1—RISK MANAGEMENT

Risk management embodies the program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, and reputation), organizational assets, staff, and other organizations. This includes establishing the context for risk-related activities, assessing risk, responding to risk once it is determined, and monitoring risk over time. A POA&M, also referred to as a corrective action plan, is a management tool for tracking the mitigation of cybersecurity program and system-level findings and weaknesses. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

The Department has developed a comprehensive governance structure and organization-wide risk management strategy and program that include comprehensive agency policies and procedures consistent with OMB policy and applicable NIST guidelines. Specifically, we found that the Department and FSA have instituted Continuous Security Authorization and Ongoing Security Authorization programs, respectively.

The Department also established a Cybersecurity Risk Management Framework that satisfies Federal security compliance and regulatory mandates by emphasizing communication at all levels and repeatable risk-based decision processes and promoting transparency in decisions. The framework also provides the mechanisms necessary for information assurance and security to be fully integrated into the Department's business processes. Risk assessments (formal or informal) are conducted at various steps in the Risk Management Framework, including (1) information system categorization, (2) security control selection, (3) security control implementation, (4) security control assessment, (5) information system authorization, and

(6) security control monitoring (continuous monitoring). Further, a Privacy Threshold Analysis is performed to determine whether a system collects, maintains, or processes personally identifiable information and whether further privacy documentation is required. This includes a Privacy Impact Analysis that effectively documents that privacy controls are implemented as appropriate to satisfy the privacy requirements set forth in the Privacy Act of 1974, the E-Government Act, OMB privacy-related policies, and NIST standards.

For Continuous Security Authorization and Ongoing Security Authorization, the certifying agent (the Chief Information Security Officer) and the independent assessment team will communicate security risks to the system owner and Information System Security Officer in formal security authorization deliverables such as a Security Assessment Report and POA&M. The Chief Information Security Officer also briefs security risks to the Chief Information Officer, Deputy Chief Information Officer, and the authorizing official. If the security risks pose a high enough threat, the Chief Information Officer also briefs them to the Chief Operating Officer's office.

We determined that the Department maintains an active system inventory (including organization and contractor operated systems, as well as cloud environments) for systems that have and have not been enrolled in their Continuous Security Authorization programs. OCIO maintains its system documentation in the Cyber Security Assessment and Management system, and FSA maintains its documentation in the Operational Vulnerability Management Solution.[9]

We also found that the Department and FSA established policy and a process for remediating and tracking security risks through the POA&M process.[10] Once approved by the Information System Security Officers, POA&Ms are entered into Cyber Security Assessment and Management system and the Operational Vulnerability Management Solution for the Department and FSA, respectively. The POA&M tracking and remediation is the primary responsibility of the Information System Security Officer and system owner. We also found that Information System Security Officers meet weekly to discuss each POA&M and the status of the remediation, biweekly to discuss high-level issues, and quarterly to discuss trending issues. Although we found the Department and FSA have a process for Information System Security Officers and system owners to track and remediate POA&Ms, the Information System Security Officer and system owners should also accurately preserve the integrity of the data quality regarding assignment and completion of POA&Ms to assist with ensuring the process is operating as intended.

Review of the Department's and FSA's Security Authorization Programs

We reviewed OCIO's Continuous Security Authorization and FSA's Ongoing Security Authorization programs and noted that they have a defined and implemented a continuous security authorization process that ensures systems are scanned and system documentation is up-to-date. In addition, we also confirmed that OCIO and FSA have a risk scoring methodology for

[9] By December 2016, FSA plans to migrate its system documentation to the Cyber Security Assessment and Management system.

[10] OCIO-01 Handbook, "Information Assurance Cyber Security Policy," August 2014; U.S. Department of Education Plan of Action and Milestones Guidance, issued in 2013; and FSA Management of POA&Ms, December 2015.

the Continuous Security Authorization and Ongoing Security Authorization programs, respectively.

OCIO's Continuous Security Authorization Program

We determined that the OCIO established a comprehensive and uniform approach to performing security control assessments for its information systems as identified in the Department's "Security Assessment Standard Operating Procedure." This process incorporates standards from Departmental, OMB, NIST, and FISMA guidance. OCIO personnel conduct information system self-assessments to support Continuous Security Authorization decisions during the operations and maintenance phase of the system lifecycle to ensure security controls are effective and continue to be in the operational environment. OCIO personnel test and assess at least one-third of these controls annually. The Chief Information Security Officer and Information System Security Officer work with the system's subject matter experts to plan for completing self-assessment activities. This includes input from artifacts such as the privacy threshold analysis, privacy impact assessment, system security plan, configuration management plan, contingency plan and test results, and incident response plan and test results.

A security control assessment is performed that includes (1) a site evaluation; (2) technical security assessments (including vulnerability scans and component testing); (3) NIST SP 800-53 requirements testing; (4) documenting self-assessment results; (5) performing an independent review of the self-assessment results and evidence; (6) documenting the results of the findings; (7) reviewing findings with appropriate stakeholders; and (8) submitting final findings to the independent verification and validation component to establish POA&Ms. Once complete, the security assessment team performs system scans every 30 days and analyzes the results to ensure that POA&Ms are cleared. If POA&Ms are not cleared, the security assessment team escalates by sending a noncompliance notification to the system owner and the Chief Information Security Officer.

FSA's Ongoing Security Authorization Program

FSA established an Ongoing Security Authorization process to oversee and monitor of the security controls in its information systems on an ongoing basis, inform the authorizing official when changes occur that might affect the security of a system, and inform risk-management decisions. This ensures that controls are in place, operate effectively, and are updated when threats, vulnerabilities, or environmental changes make the controls ineffective. When FSA identifies ineffective security controls, FSA remediates them by establishing POA&Ms and retesting remediation actions throughout the Ongoing Security Authorization process.

Enrollment in the Ongoing Security Authorization program occurs only after a system security authorization has been completed and the system has been granted an Authorization to Operate. Once in the program, a test plan is created that addresses which security controls for the system will be evaluated and the frequency of the testing[11]. All controls are tested at least once every 3 years. A security control assessment is performed of the technical, management, and operational security controls in accordance with FSA's monitoring strategy. The ongoing security controls

[11] Control testing can occur quarterly, annually, or triennially (every 3 years).

assessment is comprises manual testing, automated controls testing, and penetration testing. FSA prepares a schedule of systems to be tested on a continuous basis during each year. If a system is undergoing changes to its environment that require scanning, the Ongoing Security Authorization team leverages any scan results from up to 60 days before the start of quarterly security control testing. The Ongoing Security Authorization assessment team executes the Ongoing Security Authorization Test Plan and records the results in a Preliminary Findings Report and an Ongoing Security Authorization Quarterly Control Testing Report. Once system stakeholders are out-briefed, they have 10 business days to remediate the issues. We also found that FSA provides security status reports to the authorizing official and other senior leaders within the organization regarding the security state of the information system, including the effectiveness of deployed controls.

At the end of quarterly Ongoing Security Authorization testing, the Ongoing Security Authorization team lead briefs the Chief Information Security Officer on the past quarter's activities, discussing key vulnerabilities, findings, trends, mitigation strategies, and recommendations. The briefing identifies trends, provides an overall FSA risk rating based on the risk profiles of all FSA systems in the Ongoing Security Authorization program, and makes recommendations to improve security across the FSA enterprise. The Chief Information Security Officer signs the "Quarterly Authorization to Operate" Memorandum for all systems in the program that achieve acceptable risk levels and are approved for continued operation.

Risk Scoring Methodology

During the Continuous Security Authorization process walkthrough, OCIO demonstrated that it established a risk scoring methodology. OCIO uses System Risk is used to prioritize the recommendations associated with the system findings. An independent verification and validation team performs system scans that result in findings that the team used to populate a risk scoring worksheet. The security assessment team analyzes NIST SP 800-30, "Risk Management Guide for Information Technology Systems," and identifies all known threat sources and maps them to threat actions. The security assessment team determines the likelihood of occurrence based upon the number of threat sources and threat events that would exploit a given vulnerability and determines the system impact of each vulnerability. The security assessment team determines the risks each security control finding poses to the information technology system as a system risk score. Finally, team evaluates the overall risk associated with operating the system based on factors such as (1) Federal Information Processing Standards 199 system categorization; (2) number of high-, moderate-, and low-risk findings; (3) number of findings identified by control family (Technical, Operational, Management classes); and (4) overall number of findings for the system.

Security Package Testing

As part of our analysis of the Continuous Security Authorization and Ongoing Security Authorization programs, we reviewed security packages for the five high-value asset systems and one cloud system selected for this year's review. For FSA, we reviewed the COD system, Ombudsman Case Tracking System (a cloud system), and Person Authentication Service (PAS). For OCIO, we reviewed the Education Security Tracking and Reporting System (EDSTAR), the Education Central Automated Processing System (EDCAPS), and the Case and Activity Management System (CAMS). Our review of each system's security plan, security assessment report, POA&M, and contingency plan found no discrepancies, and the plans and reports were consistent with the requirements of each system's respective security authorization programs. In addition, as part of the Department and FSA's continuous security authorization process, for our sample of five high-value[12] asset systems and one cloud system, we found that system interconnections were identified for each system.

METRIC DOMAIN 2—CONTRACTOR SYSTEMS

We found that the Department has established a program to oversee systems operated on its behalf by contractors or other entities, including other government agencies, managed hosting environments, and systems and services residing in a cloud external to the organization, defined by comprehensive agency policies and procedures that address OMB policy and applicable NIST guidelines. However, because the Department operates in an environment in which most of its systems are contractor-operated, the Department needs to ensure it provides sufficient oversight to remediate the system-related weaknesses identified in our report whenever they involve contractors.

According to OCIO and FSA, contractor systems follow the same policies and procedures that are required by agency systems. Specifically, Departmental Handbook OCIO-01, "Information Assurance/Cybersecurity Policy," August 2014, establishes cybersecurity policy for all IT assets and services operated within or on behalf of the Department. This policy is based on statutory and executive directive requirements that include Federal laws and regulations, Presidential Directives and Executive Orders, NIST Special Publications 800 Series, NIST Federal Information Processing Standards, OMB Circulars, and the Department of Homeland Security policy. OCIO-01 applies to all Departmental personnel and contractor staff, as well as IT resources and data owned, managed, or operated on behalf of the Department. As specified, all personnel and support contractors must be familiar and comply with policy contained in OCIO-01.

For external cloud computing services, the OCIO established the "Cloud Computing Strategy," dated January 2015. This document describes the strategy for expanding the use of cloud computing in accordance with OMB's "Federal Cloud Computing Strategy." FSA also established the "Cloud Security Standard Operating Procedure," dated August 2015. This standard operating procedure explains how FSA addresses cloud computing to ensure that cloud services meet Federal requirements for security.

For the system authorization process, contractor systems must ensure the required security controls are implemented and monitored continuously. This includes the Department's Continuous Security Authorization process, which allows for the ongoing monitoring and authorization of systems. For FSA, contractors are expected to participate, perform, and formulate the required security controls testing and documentation as part of the Ongoing

[12] OMB Memorandum M-16-04, October 30, 2015, states that high-value assets are those assets, systems, facilities, data and datasets that are of particular interest to potential adversaries. These assets contain sensitive controls, instructions or data used in critical Federal operations, or they house unique collections of data (by size or content) making them of particular interest to criminal, politically-motivated, or state-sponsored actors to either directly exploit the data or cause a loss of confidence in the U.S. Government.

Security Authorization. For OCIO, system-related (including contractor systems) documentation has been migrated from the Operational Vulnerability Management Solution to the Cyber Security Assessment and Management system. As of January 2016, Cyber Security Assessment and Management system was deemed the system of record for OCIO. For FSA, its system documentation still remains in the Operational Vulnerability Management Solution. However, FSA expects its system documentation to migrate to the Cyber Security Assessment and Management system by December 2016.

We also found that the Department established and implemented a process to ensure that contracts, statements of work, and solicitations for systems and services include appropriate information security and privacy requirements. According to OCIO and FSA, contractor systems are required to comply with Departmental requirements and Federal guidelines as it relates to securing systems. Typically, agreements are based on the contracts between the organization and the vendor or contractor. Within the contract, specific security language is added that speaks to the security requirements, as well as security documentation that the contractor needs to provide. This includes compliance with FISMA, OMB Circular A-130 Appendix III, Homeland Security Presidential Directives, NIST standards and guidance, and Federal Risk and Authorization Management Program requirements and guidance. Security requirements can also include, but are not limited to the successful security authorization of a system, receipt of a full Authorization to Operate before being granted operational status, performance of annual self-assessments of security controls, annual contingency plan testing, performance of vulnerability scans, updates to all information systems security documentations as changes occur, and other continuous monitoring activities. For contractor systems that are hosted in a virtual or cloud environment, the Department relies on the Federal Risk and Authorization Management Program process since it is an already established system.

Managing of contractor systems requires the continuous monitoring of contractor performance and compliance with contract requirements. Contractor systems that are operated on behalf of the Department must comply with Federal requirements. To determine whether contracts include specific language related to Federal requirements that contractors are supposed to incorporate in the systems, we selected two systems from our sample of systems to perform our review. Specifically, we reviewed the contract documentation for PAS (Government-owned) and Ombudsman Case Tracking System (cloud-based and contractor-owned) to determine the existence of security requirements. Per our review of the contracts, we identified several sections within both contracts that speak to security requirements. Specifically, we found language that requires:

- cloud software to comply with the Federal Risk and Authorization Management Program;
- reporting of security incidents impacting data or operations, including breaches of personally identifiable information;
- cryptographic protections to comply with Federal Information Processing Standards Publications standards;
- following the Department's and FSA's incident response policy and reporting procedures;
- applications and infrastructure to be compatible and comply with Internet Protocol Version 6;

- compliance with Trusted Internet Connection requirements documented in the U.S. Department of Homeland Security's Trusted Internet Connection Reference Architecture document;
- compliance with FISMA on authorized artifacts and responding to FISMA-related data calls;
- solutions to comply with the security authorization process as outlined in NIST, as well as supporting OCIO policies, standards and procedures; and
- access management controls to comply with NIST standards.

For measuring, reporting, and monitoring security performance, contractor systems follow the POA&M process for tracking and remediating vulnerabilities, consistent with the process followed by agency systems. When a third-party (such as a third-party assessment organization) performs vulnerability scans, the Department requires the contractor to provide supporting documentation, such as an assessment report or scan results. The Department relies on the Information Systems Security Officers and system owners to validate the results, and if they identify vulnerabilities, ensure that POA&Ms are created. This process is indicative of what is required of agency systems in establishing security documentation, maintaining an authorization to operate, and mitigating any identified vulnerabilities as discussed in the Risk Management metric domain. Based on our analysis performed for the Risk Management metric domain, we verified the completion of the required security documentation for both the COD system and Ombudsman Case Tracking System in accordance with Federal requirements. Performance is also measured and tracked based on service level agreements and performance.

SECURITY FUNCTION 2—PROTECT

The "Protect" security function is comprises the Configuration Management, Identity and Access Management, and Security and Privacy Training metric domains. Based on the maturity model scoring, we determined that the Department's Protect security function scored 7 points and is at Level 2: Defined, which is categorized as being not effective. Although the Department and FSA satisfied many of the maturity model indicator metrics in each of the three areas, we identified instances where the maturity model indicator metric of "Consistently Implemented" was not being met.

We categorized the Department and FSA as being Defined, for this security function due to our findings in the three metric domains. For example, in configuration management, we found (1) select policies and procedures were not current with National Institute of Standards and Technology and Departmental guidance, (2) appropriate application connection protocols were not being used, and (3) the Department was unable to prevent unauthorized devices from connecting to the network. All three findings were repeat findings from our FY 2015 FISMA audit and continue to exist. Through our vulnerability assessment testing, we found that the Department and FSA's controls over Web applications, as well as the application's network infrastructure needs improvement. Specifically, the implementation and management of the technical security architecture supporting the Department's and FSA's applications requires strengthening to more effectively restrict unauthorized access to information resources. Further, OCIO and FSA did not implement remedial actions for previously identified security weaknesses and did not establish a proactive enterprise-wide process to fix similar vulnerabilities identified during previous audits.

For Identity and Access Management, we performed database management assessments that identified vulnerabilities, configuration errors, rogue installations, and access issues for databases residing in the CAMS, EDSTAR, PAS, and COD environments. Further, we found that two-factor[13] authentication for non-privileged users is not effectively implemented and external network connections did not use two-factor authentication—another repeat finding from the FY 2015 FISMA audit. We also found that although the Department established processes and controls to ensure an effective Security and Privacy Training program, we identified an area in which the Department can improve its assessment of people with significant security and privacy responsibilities.

As described in the maturity level scoring description, because the Department and FSA completed all metrics designated as Level 1:Ad-hoc, and met half or greater of all metrics designated in Level 2: Defined, as a result, the Protect security function scored at Level 2: Defined.

In prior years' reporting, the metric domain, remote access was reported as a separate metric area. However, for FY 2016 FISMA reporting, remote access metric questions are incorporated into the Identity and Access Management metric domain area.

<u>METRIC DOMAIN 3—CONFIGURATION MANAGEMENT</u>

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 found that the Department and FSA established a configuration management program that includes comprehensive agency policies and procedures consistent with OMB policy and applicable NIST guidelines. We reviewed 22 policies and procedures relating to OCIO and FSA's configuration management program and noted that 19 conformed with NIST SP 800-53, Revision 4, CM-1, "Configuration Management Policies" and Procedures, and NIST SP 800-128, "Guide for Security-Focused Configuration Management of Information Systems."

The Department and FSA established a configuration control process to ensure all changes to the general support system and major applications are properly requested, evaluated, and authorized. Examples of changes include (1) firewall changes, (2) domain name system changes, (3) network changes, (4) server patching, (5) desktop deployments, (6) granting administrative privileges, (7) application updates, and (8) emergency changes in response to high-priority incidents. Although emergency changes are not required to undergo the entire change control process, they must be properly documented and authorized.

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

As part of the change control process, system configuration baselines[14] are required to identify the current design and functionality of a general support system or major application, including the identification of servers, workstations, and software applications currently being used in the production environment and the specific configuration settings for each. OCIO's Information Assurance Services develops security configurations for the Department's server, desktop, and network infrastructure environment. Each system and device is required to be re-baselined annually.

System configuration baselines are identified in system security plans, and system owners must identify what baselines are necessary for their systems. FSA also uses the Defense Information Systems Agency Security Technical Implementation Guides to identify how devices should be configured to show what is allowed and what is not allowed, as well as network operating standards guidelines. Both the Department and FSA validate baseline configuration compliance by monthly system scanning. In addition, both retain previous versions of baseline configurations to support rollback.

The Department and FSA maintain hardware and software inventories in the system's configuration management plan, as well as in the configuration management database. In addition, FSA stated it deploys sensors on its network to identify anomalies (items not found in the configuration management database) and receives alerts each morning identifying hardware and software not functioning normally within the parameters of the network.

For proposed or actual changes to hardware and software baseline configurations, the Department performs risk evaluations and vulnerability scans. When the Department identifies vulnerabilities, it creates a Risk Acceptance Form. A Risk Acceptance Form is valid for one year and if the Department cannot remediate a vulnerability within that timeframe, it creates a POA&M. FSA follows a similar production readiness review to determine current vulnerabilities and develop a timeline for remediation before going into production.

We found that the Department and FSA established a decommissioning and disposal process for IT hardware. To validate this process, we visited Dell Services Federal Government Warehouse and performed an inventory-to-floor test where we judgmentally selected 17 assets from the Department's April and May 2016 Inventory Sanitization Reports. We verified that all 17 assets (1) physically existed in the warehouse (2) were documented in the warehouse records and (3) were signed by both Department asset management personnel and warehouse employees as being in the warehouse.

We also verified that the Department and FSA established a software patching process. For each system patch or update, a work order and change request is required, and the Change Approval Board approved it. All change requests must have a risk assessment to determine the potential impact, contain details of what the patch addresses and the targeted servers, and identify a back-out plan. Patching must be completed on development servers, and a peer review and manager must sign-off before implementation on the production servers.

[14] A system configuration baseline identifies the system architecture, system characterization, hardware, software, and system library.

Despite the existing processes and procedures and progress made in areas of the configuration management program, we still identified significant weaknesses in the program. Some weaknesses have been persistent for years, despite the Department's and FSA's efforts to correct them, whereas others are weaknesses we identified for the first time.

Issue 3a. Configuration Management Policies and Procedures Were Not Current With NIST and Department Guidance (Repeat Finding)

Although the Department established configuration management policies and procedures, not all of its policies and procedures had been timely updated in accordance with current NIST and Department guidance. For example, OCIO-01, "Handbook for Information Assurance Security Policy, OCIO Information Technology Security Risk Assessment Procedures," and "Cybersecurity Risk Assessment and Authorization Guide" were updated. However, of the 22 policies the Department and FSA established for configuration management, the following 3 were outdated (ranging from 6 to 12 years overdue), and did not reflect current requirements:

1. OCIO-08, "Handbook for Software Management and Acquisition Policy," 2004;
2. "Information Technology Security General Support System and Major Applications Inventory Guidance (Version 1.0)," 2009; and
3. OCIO 1-106, "Administrative Communications System Departmental Directive—Lifecycle Management Framework," 2010.

NIST SP 800-53, Revision 4, CM-1, requires agencies to develop, disseminate, and review and update formal, documented configuration management policies and procedures as frequently as the organization determines such revisions are needed.[15] OCIO defines this frequency as annually. OCIO did not update these three configuration management policies and procedures because it had not established a timely internal review and approval process.[16] NIST guidance and industry standards have been revised significantly since OCIO last updated its policies and procedures. As a result, OCIO's policies and procedures may not address current risks in the environment and may not reflect the Department's current IT infrastructure. We identified this condition as part of our FY 2014 and 2015 FISMA audits. However, it is important to note that in the areas we reviewed, we did not identify instances where Department information security practices were out of compliance with Federal requirements, even when policies had not been updated.

Issue 3b. The Department Was Not Using Appropriate Application Connection Protocol (Repeat Finding)

During the FY 2015 FISMA audit, we identified several authorized connections that used outdated secure connection protocols. The Department concurred with the findings and introduced planned corrective actions to mitigate the known risks. However, we found that the Department continued to use outdated secure connection protocols for many of its connections. Specifically, out of the 214 Department authorized active connections we tested, 66 (30 percent) failed to adhere to the mandated encryption standards. NIST SP 800-52, Revision 1,

[15] Within this section and throughout this report, the two letter abbreviations with a number (such as CM-1) refer to a specific control assigned by NIST.
[16] See our "Other Matters" section of the report.

"Guidelines for the Selection, Configuration and Use of Transport Layer Security (TLS) Implementations," requires agencies discontinue the use of the Secure Socket Layer Version 3 (SSLv3) protocol and implement TLS version 1.2. It further states that Government-only applications must be configured at a minimum to support TLS version 1.1 and should be configured to support TLS version 1.2 whenever possible. The Department did not restrict the use of non-secure SSLv3 connection to its network and did not take the necessary steps to ensure only recommended secure TLS connections were used.

Per the Department's policies, if the Department decides to accept the risks with identified controls weaknesses or vulnerabilities, it must complete and submit a Risk Acceptance Form. We reviewed all Risk Acceptance Forms the Department and FSA provided, and we did not find any forms that related to the use of SSLv3 or TLSv1.0 for the specific active connections. The transition from the SSLv3 to TLS connection would help safeguard users by providing a secure connection. Despite committing to address this issue last year, the Department has continued to use vulnerable protocols and users could still expose systems to a number of vulnerabilities and exploits, including man-in-the-middle attacks that could jeopardize Department resources.[17]

Issue 3c. The Department Was Unable to Prevent Unauthorized Devices Connected to Its Network (Repeat Finding)

The Department had no mechanism to restrict the use of unauthorized devices that are physically connected on its network. The Department plans to use a network access control[18] solution to account for and control systems, along with peripherals on its network. We originally identified this issue in our FY 2011 FISMA report, and the Department responded that the network access control solution would be operational by March 2013. We identified the same condition in our FY 2014 FISMA report, and the Department provided a revised completion date of September 2015. According to the Department, in February 2016, the ability to restrict unauthorized access was enabled and operational. However, in June 2016, our testing showed that the network access control solution was not able to restrict our access. We were able to connect to the Department's network and gain access to a number of internal resources via user credentials on a computer that was not Government-furnished equipment.

According to NIST SP 800-46, Revision 1, "Guide to Enterprise Telework and Remote Access Security," it is the organization's responsibility to assume that client devices will become infected and to plan their security controls accordingly. In addition to using appropriate antimalware technologies from the organization's secure configuration baseline, such as antimalware software on client devices, organizations should consider the use of network access control solutions that verify the security posture of a client device before allowing it to use an internal network.

Failure to restrict unauthorized devices could allow malicious users to bypass two-factor authentication, obtain the Department's Internet protocol addresses, and gain access to Department internal resources.

[17] 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.

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

Issue 3d. The Department's and FSA's Controls Over Web Applications Need Improvement

As part of our technical security vulnerability testing for this year's FISMA audit, we performed Web application testing for all 5 of our high value asset systems—CAMS, COD, EDCAPS, EDSTAR, and PAS. We found that the Department and FSA need to better implement and manage the technical security architecture that supports their applications to more effectively restrict unauthorized access to information resources. We assessed application security, and found that the Department and FSA have effectively implemented multiple controls (such as network segmentation, endpoint protection, firewalls) for protecting information resources. However, we identified several areas in which the Department could improve its security architecture could further enhance the Department's overall security. For example, we identified instances of (1) cross-site scripting (using information to impersonate the user), (2) cross-site request forgery (forcing users to modify account settings without their consent), (3) lack of ClickJacking[19] defense, (4) verbose error messages (which unintentional leak application information), (5) external service interaction (which could induce an application to interact with an arbitrary external service), (6) parameter manipulation (obtaining access to data that should not be visible to a user), and (7) privilege escalation.[20]

We also tested the COD application during our FY 2014 FISMA audit. Based on the results of our testing, we reported several vulnerabilities. We categorized some of the vulnerabilities as high severity with an expectation that they should be addressed immediately. However, during this year's testing of the COD application, we noted that the same vulnerabilities we identified in the FY 2014 FISMA report were still present and the Department had not yet mitigated them.

OCIO and FSA did not correct previously identified security weaknesses and did not establish a proactive enterprise-wide process to fix similar vulnerabilities identified during previous audits. NIST SP 800-53, Revision 4, SI-2, "Flaw Remediation," requires the Department to address any security weaknesses identified. Poor system configuration management practices increase the potential for unauthorized activities to occur without being detected and could lead to potential theft, destruction, or misuse of Department data from both internal and external threats. We provided detailed information on the vulnerabilities to OCIO and FSA for remediation, and we remain concerned that these severe vulnerabilities have not been previously addressed.

Issue 3e Network Infrastructure Supporting Department and FSA Systems Need Improvement

We conducted technical security vulnerability testing of the Department's application infrastructure (hosting CAMS, EDCAPS, EDSTAR, and PAS), as well as the supporting infrastructure components of COD. These are hosted at Dell and Total System Services, Inc., respectively. We found the Department and FSA need to better implement and manage the technical security architecture supporting the infrastructure that hosts their applications to more

[19] ClickJacking allows an attacker to use transparent or opaque layers to trick users into clicking on buttons or other controls that trigger state changing operations.

[20] We will also provide the results of our Web application testing in a Council of the Inspectors General on Integrity and Efficiency OIG community report.

effectively restrict unauthorized access to information resources. We assessed network security and we found that the Department and FSA have effectively implemented multiple controls (such as network segmentation, endpoint protection, firewalls) for protecting information resources. However, we identified several areas where improvements in the security architecture could further enhance the Department's overall security. Many of the infrastructure vulnerabilities discovered at the Total System Services, Inc., and Dell data centers resulted from missing patches and operating systems that were not properly hardened. For instance, we identified (1) open file transfer protocol ports (standard network protocol used to transfer computer files between a client and server on a computer network); (2) simple network management protocol login (certain access can shut down interfaces, reboot devices, change Internet protocol routes, and reset passwords); (3) server message block login (can authenticate using Guest account); and (4) outdated operating systems.

OCIO and FSA did not correct previously identified security weaknesses and did not establish a proactive enterprise-wide process to fix similar vulnerabilities identified during previous audits. NIST SP 800-53, Revision 4, SI-2, "Flaw Remediation," requires the Department to address any security weaknesses identified. Poor system configuration management practices increase the potential for unauthorized activities to occur without being detected and could lead to potential theft, destruction, or misuse of Department data from both internal and external threats. The select repeat conditions were similar conditions identified during our FY 2011, 2012, 2013, and 2015 FISMA audit reports. We provided detailed information on the vulnerabilities to OCIO and FSA for remediation, and we remain concerned these issues have not been corrected.

Recommendations

We recommend that the Deputy Secretary and Under Secretary require OCIO and FSA to—

3.1 Ensure that policies and procedures are reviewed and revised at least annually, or as needed. (Repeat Recommendation)

3.2 Update the outdated configuration management policies and procedures to reflect current NIST and industry standards. (Repeat Recommendation)

3.3 Immediately establish TLS 1.1 or higher as the only connection for all Department connections. (Repeat Recommendation)

3.4 Enable the network access control solution to validate and restrict personal devices from connecting to the Department's internal network. (Repeat Recommendation)

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

3.6 Ensure POA&Ms are created to remedy infrastructure vulnerabilities identified in the Dell and Total System Services, Inc., data center environments.

Management Comments

The Department concurred with the recommendations.

OIG Response

The Department's planned corrective actions, if properly implemented, are responsive to the findings and recommendations.

METRIC DOMAIN 4—IDENTITY AND ACCESS MANAGEMENT

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

We determined that the Department and FSA established an identity and access management program, including policies and procedures consistent with OMB policy and applicable NIST guidance. In September 2012, the Department developed the Identity Management Roadmap to provide a strategy to implement the Federal Identity, Credential, and Access Management capability for the Department and provide the common vision and goals that guide and integrate the Department's many cyber, identity, and information assurance initiatives and investments.

For individuals, including contractors, requiring access to organizational information and information systems, we found that the Department and FSA established processes that include signing a Rules of Behavior form, completing and verifying security awareness training before receiving network access, and recertifying security awareness training annually. We tested a sample of 25 new Federal employees who were hired from October 2015 through April 2016. We requested documentation of the employee's completed Cyber Security Awareness and Privacy Training completion certificate, signed Rules of Behavior form, and Account Request/Termination Form.[21] We found that all 25 employees had a completed Account Request/Termination Form, and 24 of 25 had a completed Cyber Security Awareness and Privacy Training certificate, and all the employees had signed the Rules of Behavior form.

The Department and FSA officials confirmed that they had procedures to terminate and deactivate accounts that no longer required access or had been dormant for 90 days. The Department and FSA terminate or deactivate accounts based on notices from Human Resources or contracting officer's representatives.

[21] As described in the Dell Services Federal Government's Standard Operating Procedure for New Hire Account Request, August 13, 2015, the Account Request/Termination Form stipulates the technology equipment and access being requested for a new employee or contractor.

The Department and FSA established a process that ensures employees are granted access to the network and applications based on least privilege and separation of duties principles. Once the employee completes the clearance process, the employee's principal office information technology coordinator determines permissions based on job functions of the new employee. These permissions are documented in the Account Request/Termination Form or the Remedy Self-Help Ticketing system. The Department and FSA follow a similar process for contractors, but the contracting officer's representative helps complete the Account Request/Termination Form. Department and FSA officials also confirmed that shared accounts are not permitted within the EDUCATE and Virtual Data Center environments.

We determined that the Department established policy and organizational responsibilities for the issuance of its media credentialing. Specifically, after an employee completes the Department's identification card application process, and a minimum background investigation is adjudicated, the employee receives a Personal Identity Verification (PIV) card.[22] We determined that the Department implemented PIV for logical access to the network in accordance with Federal guidelines. The Department also established a process for granting temporary access to the network for lost or expired PIV cards. The only exceptions the Department identified for not using PIV access are for short-term employees or employees subject to Section 508 of the Rehabilitation Act of 1973.

The Department established a process for monitoring and tracking privileged user access rights, and the principal office information technology coordinator must reevaluate and reassess that access at least annually. The principal office information technology coordinator reviews a user's privileged access rights, and in the case of denial, terminates access. Privileged users must go through the complete privileged user access process, which normally occurs at the application level.

The Department and FSA also instituted a new management tool—CyberArk Privileged Account Security—for users with privileged access to systems and network appliances. According to the CyberArk Privileged Account Security Concept of Operations, November 2015, CyberArk provides control and monitoring of privileged accounts, protecting sensitive accounts from misuse and providing assurance that such accounts are controlled and managed. One component, the CyberArk Enterprise Password Vault, protects privileged account passwords based on privileged account security policies—controlling which privileged users can access passwords and when. Another component, Privileged Session Manager, isolates, controls, and records privileged user access as activities for critical systems, network devices, and databases.

Department officials confirmed that the Department possesses the capabilities to account for and distinguish all devices and assets with Internet protocol addresses on the EDUCATE network (including hardware assets that have user accounts from those without user accounts). Additionally, during our walkthrough of the Department's Security Operations Center, Department officials provided a demonstration of how its network access control solution has the capabilities, when fully implemented, to identify hardware assets and distinguish between assets that are associated with users' accounts and those that are not. Although this technical solution has the ability to control network access, OCIO has not fully implemented this functionality yet.

[22] A PIV card is used for entry control into Government owned and leased facilities and all Department facilities and offices in headquarters, regional, field, and area offices.

For remote access sessions, we found that the Department and FSA established a time-out capability to log off users after 30 minutes of inactivity. We reviewed the results of the Department's independent testing of remote connections' timeout ability. We also reviewed the Department's and FSA's list of authorized remote connections and performed our independent validation by testing one of the connections. We confirmed that remote access sessions are timed out after 30 minutes of inactivity, requiring user re-authentication.

We found that the Department enforced a limit of consecutive invalid remote access logon attempts and automatically locked the account. According to the Department's password policy, networks, systems, and applications are configured to lock out accounts after three invalid logon attempts. To verify this capability, we reviewed the system logs and reports verifying logon attempts and account lockouts and terminations. We also found that the Department used incident reports to track and monitor invalid logon attempts of its users and is able to track and monitor the incidents where remote access was disabled. We also reviewed the "Telework Registration System Security Plan" and found that its test plan included testing lockout after three unsuccessful login attempts and time-out after 30 minutes of inactivity.

Although the Department and FSA made progress in developing their identity and access management process, we have also identified areas that need strengthening. For instance, we found that (1) the Department and FSA need to improve their controls over database management, (2) the Department did not consistently and effectively implement two-factor authentication for non-privileged users for accessing internal resources; and (3) nine external network connections did not use two-factor authentication. This last finding was a repeat finding identified in our FY 2015 FISMA audit.

Issue 4a. The Department's and FSA's Controls Over Database Management Needs Improvement

We performed database assessments that identified vulnerabilities, configuration errors, rogue installations, and access issues for databases residing in the CAMS, EDSTAR, PAS, and COD systems. These systems were also four of the five high-value asset systems we selected as part of system testing for this year's FISMA audit. Vulnerability scans identified significant security weaknesses that the Department and FSA need to address to better safeguard data stored for three of the five systems we tested. Specifically, a number of rights issues need to be strengthened to prevent unauthorized access or compromise of the confidentiality, integrity, and availability of the database information. Our scans identified vulnerabilities categorized as high, medium, and low.[23] Listed below are the results of the vulnerability assessments performed in each environment.

[23] High—if exploited, this vulnerability would yield complete control of the subject system or access to extremely sensitive data to attackers, severely disrupting system operations and integrity. Medium—while not directly leading to a system security breach, if exploited, this vulnerability may play a significant role in combination with other vulnerabilities to make pertinent system information available to an attacker. Low—a vulnerability that is unlikely in itself to lead directly to a compromise of a system, but can in some way aid an attacker indirectly in mounting attacks against the subject system.

CAMS Environment

Vulnerability scans identified significant security weaknesses that the Department needs to address to better safeguard data stored in the CAMS databases. Our scans identified seven high vulnerabilities, six medium vulnerabilities, and six low vulnerabilities. For instance, we found (1) password weaknesses (password same as login name, passwords not changed timely); (2) service packs were not current; (3) excessive permissions were granted; (4) servers were vulnerable to remote code execution; (5) remote access to servers was allowed; (6) misconfiguration allowed improper command execution; and (7) system administrator roles could be improperly granted.

EDSTAR Environment

Vulnerability scans identified significant security weaknesses that the Department needs to address to better safeguard data stored in the EDSTAR database. Our scans identified one high vulnerability, three medium vulnerabilities, and three low vulnerabilities. For instance, we found (1) password weaknesses (not changed timely), (2) excessive permissions were granted, (3) misconfiguration allowed improper command execution, and (4) system administrator roles could be improperly granted.

PAS Environment

Vulnerability scans identified significant security weaknesses that the FSA needs to address to better safeguard data stored in the PAS databases. Our scans identified 37 high vulnerabilities, 172 medium vulnerabilities, and 99 low vulnerabilities. For instance, we found (1) password weaknesses (passwords easily guessed, default passwords not changed, password not changed within allotted time, expired passwords, lock-out time not consistent with policy, password reuse not consistent with policy, password life not consistent with policy); (2) excessive account privileges; (3) privileges not correctly assigned; (4) a user role that did not require a password; and (5) a non-standard account was found with a database administrator role.

In addition, because of access issues, we were not able to scan the operating system to validate its security posture and patching level. Although the OIG testing team worked with FSA personnel to try and resolve the access, we could not successfully access the operating system during our testing. Therefore, our results could not provide the complete security posture of the PAS database environment.

COD Environment

Vulnerability scans identified significant security weaknesses that FSA needs to address to better safeguard data stored in the COD database. Our scans identified 5 high vulnerabilities, 29 medium vulnerabilities, and 9 low vulnerabilities. For instance, we found (1) logon attempt parameters were not set correctly; (2) account privileges were not adequately controlled; (3) password weaknesses (password strength, password expiration outside of parameters, lockout time value set low, password reuse parameter not set correctly, password change frequency not correctly set); (4) auditing system not configured to record connection attempts; (5) excessive account permissions; (6) audit data records not encrypted; and (7) nonstandard account granted a database administrator role.

NIST SP 800-53, Revision 4, provides guidelines and security controls that organizations need to follow regarding access controls, audit and accountability, configuration management, identification and authentication, and system integrity.[24] The Department and FSA have not taken the necessary steps to address access, audit, configuration, identification, authentication, and system integrity requirements on their respective systems. Failure to regularly validate the security posture of databases could lead to data leakage and exposure.

Issue 4b. Lack of Enforcement of PIV for Non-Privileged Users

The Department did not consistently and effectively implement two-factor authentication for non-privileged users for accessing internal resources. Specifically, the Department did not meet the goal of using a PIV or NIST Level of Assurance 4 credentials for at least 85 percent of its Federal employees and contractors. As identified in the "Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government," October 2015, Federal agencies should continue to target the Administration Cybersecurity Cross-Agency Priority goal of strong authentication for 85 percent of unprivileged users. Under the FY 2016 FISMA Metrics, two-factor authentication is considered consistently implemented if used for at least 85 percent of non-privileged uses. During 2016, the Department reported 7,373 unprivileged user network accounts. Of these 7,373 accounts, the Department reported 6,413 (or 82 percent) were required to log onto the network with a two-factor PIV or NIST Level of Assurance 4 credential.[25] Further, OCIO was unable to provide evidence to support the reported 6,413 accounts; therefore, we were unable to validate the extent to which the Department uses two-factor authentication.[26]

Allowing access to internal resources with only a user name and password weakens the Departments IT security program. Without a secondary authentication factor, the Department is more vulnerable to sophisticated social engineering attacks and password attacks that attempt to gain access to users' authentication credentials. Also, the likelihood of such attacks is high; if such attacks are successful, they can have an adverse impact on the confidentiality, integrity, and availability on Department data and resources.

Issue 4c. Nine External Network Connections Did Not Use Two-Factor Authentication (Repeat Finding)

The Department and FSA did not consistently enforce the use of two-factor authentication for users that connect to Department resources remotely. We requested a list of all Department and FSA remote connections. Of the 46 remote connections the Department identified, we found that 9 (19 percent) were not configured to use two-factor authentication. These remote connections were configured to connect to Department resources using one-factor authentication that was limited to a user name and a password.

[24] Specifically, Account Management (AC-2), Least Privilege (AC-6), Unsuccessful Logon Attempts (AC-7), Remote Access (AC-17), Audit Events (AU-2), Protection of Audit Information (AU-9), Configuration Settings (CM-6), Identification and Authentication (Organizational Users) (IA-2), and Flaw Remediation (SI-2).

[25] According to NIST SP 800-63-1, "Electronic Authentication Guideline," Level 4 is intended to provide the highest practical remote network authentication assurance.

[26] In addition, the Department could not provide support for the number of privileged users who used PIV credentials.

OMB 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," specifies that remote access is allowed only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. NIST SP 800-53, Revision 4, requires the use of two or more factors to achieve authentication. The factors are defined as something you know (for example, password or personal identification number); something you have (for example, cryptographic identification device or token); or something you are (for example, biometric). The Department and FSA failed to enforce the use of two-factor identification for its remote connections and allowed users to sign on with only a username and password. Allowing users to sign on without two-factor authorization could expose data and user accounts and allow an intruder to access the network, leading to cyberattacks. Also, not requiring external users to use two-factor authentication places the systems and the data at risk for exposure from unauthorized users. We identified similar conditions in our FYs 2014 and 2015 FISMA audits. Although the Department's corrective action plans stated that this finding was addressed in December 2015, we still found remote connections that did not require two-factor authorization.

Recommendations

We recommend that the Deputy Secretary and Under Secretary require OCIO and FSA to—

4.1 Enforce two-factor authentication on all remote connections. (Repeat Recommendation).

4.2 Create POA&Ms to remedy database vulnerabilities identified in the CAMS, EDSTAR, PAS, and COD environments.

4.3 Resolve access issues to ensure the OIG can complete future vulnerability assessments for the PAS environment.

4.4 Enforce two-factor authentication for all users (Federal employees, contractors and external business partners) with unprivileged user network accounts that access internal resources.

4.5 Develop a reporting mechanism that allows the Department to maintain consistent reporting of unprivileged user accounts and network authentication statuses.

Management Comments

The Department concurred with recommendations 4.1, 4.2, 4.3, and 4.5. However, the Department only partially concurred with recommendation 4.4. In its response to recommendation 4.4, the OCIO noted that the Department has established and implemented a policy to enforce two-factor authentication. Also, for Q4 of FY 2016, the Department stated that it is at 96% enforcement of two-factor authentication for unprivileged accounts. The Department plans to develop a plan to address users who authenticate via alternate two-factor technologies outside of PIV. The planned completion date is February 28, 2017.

OIG Response

The Department's planned corrective actions, if properly implemented, are responsive to the finding and recommendations. OIG will validate the percentage reported for Q4 enforcement of two-factor authentication for unprivileged users during its FY 2017 FISMA audit.

METRIC DOMAIN 5—SECURITY AND PRIVACY TRAINING

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

We found that the Department established a security and privacy awareness training program defined by comprehensive policies and procedures that incorporate OMB policy and applicable NIST guidelines. Specifically, the Department's program is defined in OCIO-01, "Handbook for Information Assurance/Cybersecurity Policy," and the Department's "Information Technology Security Training and Awareness Program" guidance. These documents address the purpose, scope, roles, responsibilities, management commitment, coordination, and compliance of the Department's security training program.

The Department developed security and privacy awareness training material that promotes user awareness regarding phishing, malware, social engineering, and insider threats in accordance with Federal requirements. To measure the effectiveness of its security and privacy awareness training, the Department conducts organized exercises, such as sending out phishing emails, and documents the results.

The Department tracks the security and privacy awareness training for its Federal employees and contractors using the Talent Management System and Security Touch, respectively. Security training can be taken either online through the Talent Management System and Security Touch, or through live sessions the Department administers. For live sessions, attendance is verified through a sign-in sheet or signed Rules of Behavior document (for new employees) and is manually inputted into the respective tracking system. Both tracking systems have databases that track users' training completion status. As of April 2016, the Talent Management System listed a total of 4,190 Federal employees and Security Touch listed 4,651 contractors. We selected a random sample of 156 users (78 Federal employees and 78 contractors) to determine whether the Department maintained the appropriate security and privacy awareness training documentation for users identified as completing this training. We validated that the Department maintained security and privacy awareness completion certificates for all 156 users.

We also found that the Department has established processes to track the specialized security and privacy awareness training for Federal employees and contractors. Personnel that require specialized training are also tracked in the Talent Management System and Security Touch. Information system security officers are responsible for identifying Department employees and contractors with significant information security responsibilities and track the status of their training, which includes specialized or role-based training.[27]

Although the Department established processes and controls to ensure an effective security and privacy training program, we identified the following area where the Department can improve its assessment of individuals with significant security and privacy responsibilities.

Issue 5. Assessment Needed For Individuals With Significant Security Responsibilities

We found that the Department did not establish a process for assessing the knowledge, skills, and abilities of individuals with significant security responsibilities. The Department confirmed that it had not developed an assessment process for individuals with significant security responsibilities as part of its security program. NIST SP 800-50, "Building an Information Technology Security Awareness and Training Program," states that an organization must conduct a needs assessment to determine the organization's awareness and needs. The organization must also create individual development plans for users with significant security responsibilities. By not assessing the knowledge, skills, and abilities of individuals with significant security responsibilities, the Department could not develop security training content to close identified gaps and enable these individuals to effectively perform their duties.

Although we found that Department and FSA do not currently have a process to assess the knowledge, skills, and abilities of individuals with significant security responsibilities, we identified additional security controls outside of the required reporting metrics to ensure the effectiveness of the Department's security and privacy awareness program. Specifically, we followed up on the FY 2015 FISMA audit finding regarding new employees being required to take training before being allowed access to the Department's network. We found that the Department now requires new employees (Federal and contractor) to complete security awareness training and role-based training before being issued a PIV card, which employees use to gain access to the Department's network. Also, when an employee does not complete required annual security training, the Department sends notifications directly to the employee, the contracting officer's representative (if the employee is a contractor), and the information system security officer. If the employee does not complete the training within the required timeframe, the employee's account is locked or suspended until the employee completes the training.

Recommendations

We recommend that the Deputy Secretary require OCIO to—

5.1 Assess of the knowledge, skills, and abilities of individuals with significant security responsibilities.

5.2 Develop security training content to close identified gaps identified by the assessments.

[27] Security roles are based on definitions from National Initiative for Cybersecurity Education and Office of Personnel Management. There are about 20 to 30 roles, such as system administrators, software developers, and contracting officer's representative.

Management Comments

The Department concurred with the recommendations.

OIG Response

The Department's planned corrective actions, if properly implemented, are responsive to the finding and recommendations.

SECURITY FUNCTION 3—DETECT

The "Detect" security function comprises the ISCM maturity model. We assessed this Security Function against established maturity model criteria that focus on the program's maturity in three areas: people, processes, and technology. In FY 2015, we evaluated the ISCM program reported it at Level 1: Ad-hoc. The FY 2016 FISMA Metrics continued with the same ISCM maturity model, but clarified that the program must be at or above Managed and Measurable to be considered effective. Although we noted that the Department made some progress from the FY 2015 FISMA maturity level determination, we determined the Detect security function scored 3 points and is at Level 1: Ad-hoc, which is categorized as being not effective.

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 overall ISCM metric domain for the Department and FSA was not effective because the program met metrics only for Level 1 of the Council of the Inspectors General on Integrity and Efficiency's ISCM maturity model. Level 1 means the program is not formalized and ISCM activities are performed in a reactive manner. This was the same level at which we assessed the Department's and FSA's ISCM program during our FY 2015 FISMA audit.

Since FY 2015, the Department developed comprehensive policies and procedures for security assessments, risk assessment and authorization, ongoing security authorization, cybersecurity risk management framework, and the risk assessment and computation process. In addition, OCIO identified a number of actions taken to progress to maturity level 2, such as (1) updating the OCIO-01, "Handbook for Information Assurance/Cybersecurity Policy;" (2) finalizing the Risk Management Framework document; (3) finalizing the "Cybersecurity Risk Assessment and Authorization Guide;" (4) updating the ISCM Roadmap to reflect the Department's current status regarding the ISCM maturity model; and (5) developing a continuous monitoring plan. OCIO also informed us that the Department has increased communication through the adoption of the Risk Management Framework, which includes hosting various workshops that discuss roles and responsibilities within the Framework.

Although the Department and FSA defined how they would implement their ISCM activities, their ISCM processes, performance measures, policies, and procedures have not been implemented consistently across the organization. We note, however, pursuant to OMB requirements, agencies have until FY 2017 to fully implement continuous monitoring of security controls. Until ISCM is fully implemented, the Department and FSA will continue to rely on manual processes. We discuss additional details in the Risk Management metric domain, under the "Identify" security function.

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

The ISCM maturity model provides perspective on the overall status of information security within an agency, as well as across agencies. We assessed the Department-wide ISCM program against three categories: people, processes, and technologies.[28] The Department's and FSA's maturity levels are based on whether they meet all attributes for that level.

We determined that the Department's and FSA's ISCM program was at Level 1 of the maturity model. Specifically, we found that the Department and FSA did not meet Level 2 requirements because the Department and FSA (1) have not assessed the skills, knowledge, and resources needed to effectively implement an ISCM program (at both Level 1 and Level 2); and (2) have not defined ISCM stakeholders and their responsibilities and communicated this across the organization.

In addition, we reviewed the ISCM Roadmap and found that it contains some outdated information and does not reflect the current environment. OCIO stated that the ISCM Roadmap is under construction to reflect the Department's current maturity level. However, OCIO did not state when the new Roadmap would be available.

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

Recommendation

We recommend that the Deputy Secretary and the Under Secretary require OCIO and FSA to—

6.1 Incorporate additional measures to achieve Level 2 status for their ISCM program. In particular, implement a program that (1) assesses the skills, knowledge, and resources needed to effectively implement an ISCM program at both Levels 1 and 2 and (2) defines

[28] The continuous monitoring management metric was to be evaluated for overall progress. This metric gauges what has been accomplished and what still needs to be implemented to improve the information security program and progress across the maturity levels.

ISCM stakeholders and their responsibilities and communicate these across the organization. (Repeat Recommendation)

Management Comments

The Department concurred with the recommendations.

OIG Response

The Department's planned corrective actions, if properly implemented, are responsive to the finding and recommendation.

SECURITY FUNCTION 4—RESPOND

The "Respond" security function comprises the Incident Response metric domain. For FY 2016, the Council of the Inspector General on Integrity and Efficiency in coordination with OMB and Department of Homeland Security, developed the Incident response maturity model. The maturity model was structured with similar criterion with the focus on three core areas of the program: people, processes, and technology. Based on our evaluation of the Incident Response program, we determined the Response Security function scored 3 points and is at Level 1: Ad-hoc, which is categorized as being not effective. Specifically, the Department and FSA did not have documented policies and procedures, inconsistently implemented incident handling procedures for security events, and had not implemented incident response technologies.

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 IT services.

The Incident Response maturity model provides a perspective on the overall status of information security within an agency, and helps ensure consistency across multiple agencies. We determined that the overall incident response program for the Department and FSA was generally not effective. 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. Until this is achieved and fully implemented, the Department and FSA will continue to rely on inconsistent processes.

Issue 7. The Department and FSA's Incident Response Program Needs Improvement

We determined that the Department's and FSA's incident response programs were at Level 1, Ad-hoc of the maturity model. Our review of the Department's and FSA incident response programs were measured against three categories: people, processes, and technology. Specifically, we found that the Department and FSA:

(1) had not assessed the skills, knowledge, and resources that are needed to effectively implement the incident response program;
(2) inconsistently implemented processes for collaborating with the Department of Homeland Security, and other parties as appropriate, to provide on-site technical assistance for quickly responding to incidents;
(3) inconsistently used qualitative and quantitative measures to perform trend analysis and situational awareness
(4) had not fully implemented automated technologies that are used to respond to security incidents.

The Department and FSA have not fully developed, implemented, or enforced policies and procedures to manage an effective incident response program. Specifically, because they did not have procedures to assess the skills, knowledge, and resources, procedures were not implemented or enforceable. The Department and FSA inconsistently followed their internal procedures when reporting security incidents to OIG's Technology Crimes Division, which impacted its ability to respond to significant security events. We reviewed security incidents from October 2015 through June 2016 and found that the Department and FSA did not timely report several security incidents to OIG's Technology Crimes Division for response. Additionally, the Department and FSA are in the process of implementing automated tools that can identify devices attempting to gain access to the network and mitigate the risk of data being exposed. However, the Department and FSA have postponed the full deployment of such tools multiple times over the past few years.

OMB and NIST guidelines[29] 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 and FSA increase the chances that they will be unable to detect a compromise to their IT systems.

[29] 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.

Recommendation

We recommend that the Deputy Secretary and Under Secretary require OCIO and FSA to—

7.1 Incorporate additional measure to, at a minimum, achieve Level 2 status of the Incident Response program. In particular, (1) assess the skills, knowledge, and resources needed to effectively implement an incident response program and (2) fully implement and enforce incident response capabilities and tools.

Management Comments

The Department concurred with the recommendation.

OIG Response

The Department's planned corrective actions, if properly implemented, are responsive to the finding and recommendation.

SECURITY FUNCTION 5—RECOVER

The "Recover" security function comprises the Contingency Planning metric area. Based on the maturity model indicator scoring, we determined that the Department's contingency planning program scored 20 points and was at Level 5: Optimized, which is categorized as being effective. Specifically, the Department and FSA established policies and procedures consistent with OMB policy and applicable NIST guidelines: they maintained recovery strategies, plans, and procedures at the organization and application level; developed a comprehensive disaster recovery process; and considered supply chain threats as part of their contingency planning process.

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 found that the Department had established an enterprise-wide business continuity and disaster recovery program that included policies and procedures consistent with OMB policy and applicable NIST guidelines. Specifically, the Department and FSA use OCIO-01, "Information Assurance/Cybersecurity Policy" for continuity of operations, disaster recovery, and contingency planning. Also, they both follow the Department's "Information Technology Security Contingency Planning Procedures" for their programs. In addition, for its contingency planning, FSA incorporates the Virtual Data Center's system security plan and telecommunications plan, as well as the Virtual Data Center's supply chain management standard operating procedure.

We determined that the Department and FSA developed and maintained recovery strategies, plans, and procedures at both the organization and application level. From our sample of five high-value asset systems, we found that the Department and FSA established a contingency plan and disaster recovery plan for all five systems.[30] Specifically, we found that all five contingency plans:

- contained all the required elements,
- identified testing and maintenance activities associated with restoring the system after a disruption or failure,
- had primary and alternative telecommunication services and necessary agreements in place to permit the resumption of operations when primary telecommunications capabilities were unavailable, and
- identified an alternate storage site and provided the frequency of back-ups.

Both the Department and FSA incorporate business impact assessments into the Continuity of Operations Plan, and Disaster Recovery Plan, which are reviewed by application teams and business areas. Business Impact Assessments are used for determining tier-level recovery times and risks associated with the system. From our sample of five high-value asset systems and one cloud system, we found that all six established Business Impact Assessments.

We also determined that the Department and FSA established training program for employees involved with the disaster recovery process. These training requirements were defined within the contingency planning documents.

We determined that the Department and FSA established an annual process to plan, execute, and document disaster recovery results. For FY 2016, we attended planning meetings, as well as observed the EDUCATE disaster recovery exercise. This exercise included three of the high-value asset systems we selected for this year’s FISMA review: EDSTAR, EDCAPS, and CAMS. We determined that the recovery exercise was successfully executed, and in accordance with the documented plans and timelines. The Department and FSA encountered and resolved three issues during the exercise. During the planning and execution of the disaster recovery exercise, we noted that the Department used (1) a comprehensive test plan, (2) a disaster recovery exercise schedule, (3) a checklist for pretest activities, (4) success criteria for the exercise, (5) exercise status reports, (6) a GAP analysis document, and (7) a lessons-learned document.

The Department and FSA consider supply chain threats as part of the contingency planning process. Supply chain threats are identified in the Department’s “Information Technology Contingency Planning Guidelines” and in FSA’s “Virtual Data Center’s Supply Chain Threat Management” standard operating procedure. For supply threat changes, contingency planning documents are updated immediately and minor changes are incorporated in annual reviews. Additionally, FSA stated that supply chain threats are addressed in the Virtual Data Center

[30] We did not review contingency planning documentation for the Ombudsman Case Tracking System, which was re-architectured and migrated to a cloud solution in FY 2015. The documentation for this system did not depict the current state of the system. We will review the contingency planning documentation for the system at a later date.

system security plan, and the Department stated that supply chain threats are addressed in the EDUCATE system security plan.

OTHER MATTERS

In prior year FISMA audits, we have identified findings—most of which were repeat—where the Department's policy and guidance documents were not current with NIST and Department policy.[31] Specifically, the Department had not updated and implemented policies and guidance. Because this was a reoccurring condition, we examined the policy review and approval process to help identify areas where the Department could strengthen current practices. (See Issue 3a, "Configuration Management Policies and Procedures Were Not Consistent with NIST and Department Guidance (Repeat Finding).")

POLICY REVIEW AND APPROVAL PROCESS

At the Department, policy development involves two distinct processes—the agency-wide Administrative Communications Systems (ACS) process administered through the Office of Management, and OCIO internal process, administered through Information Assurance Services. Policies that are considered high-level and would impact stakeholders across the Department must go through the ACS process. This requires input by the union since areas or changes may impact bargaining unit employees. Under the previous ACS process with the union, Department policy finalization and approval process took up to 2 years. The Department stated that the updated ACS finalization and approval process has been streamlined for completion within 120 days. The OCIO's internal Information Assurance Services process follows the same policy development process as ACS; however, OCIO follows its own internal process for administration, where the Chief Information Security Officer and the Chief Information Officer are responsible for signing off on policies.

The Policy and Planning team, which has three members, is located in the OCIO and is responsible for developing policy and guidance relating to cybersecurity, continuous monitoring requirements, and other related security control implementation requirements. It also coordinates Department-wide cybersecurity policies regarding network and system security management, operational, and technical controls. The Department's methodology for development, review, update, and approval of cybersecurity policies, standards, guidance, processes, and memoranda is outlined in the "Information Assurance Services Cyber Security Document Development, Review, Update and Approval Process," January 2016.

During our review of the policy and guidance process, we identified areas that the Department should consider addressing to help strengthen this process and could assist in preventing repeat findings. Specifically, we found the following.

- Of the three Policy and Planning team members assigned to policy planning, development and review, two are assigned only as part-time due to other responsibilities.
- OCIO officials confirmed that policy documents include guidance, handbooks, directives, and standard operating procedures. However, according to the Chief Information

[31] (1) FY 2015 (A11P0001) Issue 2a (Repeat); (2) FY 2014 (A11O0001) Issue 1a, 2a (Repeat), 4a (Repeat), 5i (Repeat); FY 2013 (A11N0001) Issue 2b, 3a (Repeat), 5a (Repeat), 6 (Repeat), 8b (Repeat), 8e.

Security Officer, the Department has not effectively defined various document forms and no formal guidance exists that constitutes each. The Office of Management would be the program office that would define the various documents and disseminate the definitions across the Department. Per the Chief Information Security Officer, without a clear definition, staff may not recognize them as policy. Although the Policy and Planning team has reached out to the Office of Management for clarification, this issue remains unresolved.

- The Policy and Planning Branch Chief and Chief Information Security Officer both acknowledged that the policy dissemination process needs to be improved. Currently, policy is disseminated through the intranet. Once policies are uploaded, the Department expects the Information System Security Officers, system owners, and other key stakeholders visit the site to obtain current policies and procedures. The Policy and Planning Branch Chief and Chief Information Security Officer believe that disseminating policies through SharePoint would provide users easier access.

We also found that the Information Assurance Service Directorate maintains a Policy and Guidance Maintenance Priority List. The list comprises outstanding ACS Directives and Non-ACS Directives/Chief Information Officer Guidance that identifies the (1) Directive/Handbook number, (2) initial draft issuance date, (3) last date the document was signed, (4) owner/point of contact for the document, (5) most recent update to the document, (6) date the document was signed by Chief Information Security Officer, (7) document's planned date of OCIO completion, and (8) extension due date.

As of May 5, 2016, OCIO stated that 3 ACS Directives and 24 Non-ACS Directives/Chief Information Officer Guidance still needed completion. Of the 27 incomplete documents, we found the following.

- Nine (33 percent) had recently been updated (one ACS and eight Non-ACS/CIO Guidance).
- Nine (33 percent) were signed by the Chief Information Security Officer (one ACS and eight Non-ACS/CIO Guidance).
- Nine (33 percent) had a planned date of OCIO completion (one ACS and eight Non-ACS/CIO Guidance). Of the nine, we noted that one OCIO completion date was not met, and one missed the targeted OCIO completion date with no extension date identified.

To help strengthen its policy and approval process and avoid future findings, we suggest that OCIO take action on the following areas of improvement:

- Evaluate and determine whether the current staffing of the policy and process team is efficient for the policy planning, development, and review process.
- Continue to work with Office of Management to define policy documents.
- Improve policy dissemination.
- Expedite the issuance of the 24 outstanding Non-ACS/Chief Information Officer guidance documents.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine whether the Department and FSA's overall information technology security programs and practices were generally effective as they relate to Federal information security requirements. For fiscal year 2016, the Inspector General reporting metrics were organized around the five information Security Functions outlined in the National Institute of Standards and Technology'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) Contractor Systems, (3) Configuration Management, (4) Identity and Access Management, (5) Security and Privacy Training, (6) Information Security Continuous Monitoring, (7) Incident Response, and (8) Contingency Planning. For FY 2016, OIGs were also required to evaluate the maturity level for the Information Security Continuous Monitoring and Incident Response cybersecurity areas.

To accomplish our objective, we performed the following procedures:

- reviewed applicable information security regulations, standards, and guidance;
- gained an understanding of IT security controls by reviewing policies, procedures, and practices that the Department has implemented at the enterprise and system levels;
- assessed the Department's enterprise- and system-level security controls;
- interviewed Department officials and contractor personnel, specifically staff with IT security roles, to gain an understanding of the system security and application of management, operational, and technical controls;
- gathered and reviewed the necessary information to address the specific reporting metrics outlined in Department of Homeland Security's FY 2016 Inspector General FISMA reporting metrics; and
- compared and tested management, operational, and technical controls based on NIST standards and Department guidance.

Additional testing steps to substantiate identified processes and procedures included:

- system-level testing for the Configuration Management, Risk Management, and Contingency Planning metrics;
- review of the OCIO's Security Control Assessment and FSA's Ongoing Security Authorization programs;
- vulnerability assessment testing of CAMS, EDCAPS, EDSTAR, PAS, and COD web applications and infrastructure;
- testing the security incident process with simulated threats;
- verifying training evidence and completion;
- verifying credentials within the access management;
- verifying security settings for the Department data protection; and
- observing the EDUCATE disaster recovery exercise.

In June 2015, the OMB initiated the Cybersecurity Sprint that instructed agencies to implement a number of immediate high-priority actions to enhance the cybersecurity of Federal information and assets. The Cybersecurity Strategy and Implementation Plan resulted from the Cybersecurity Sprint, which identified and addressed critical cybersecurity gaps and emerging priorities and made specific recommendations to address those gaps and priorities. The Cybersecurity Strategy and Implementation Plan was designed to strengthen Federal civilian cybersecurity through specific objectives—one of which was identifying high-value assets and immediately reviewing the protections around these designated assets.[32] In response to OMB's Cybersecurity Sprint effort, the Department and FSA identified, scored, and ranked their high-value asset systems in the areas such as (1) sensitivity of information, (2) quantity of sensitive information stored or handled, (3) uniqueness of data set, (4) impact of loss or compromise, (5) system dependencies, and (6) communications support. We focused on the most critical and highly scored systems, including the six areas mentioned above. We also considered whether the system was an agency-owned or a contractor system. Lastly, we also wanted to include a cloud-based system as part of our sample.

The table below lists the judgmentally selected systems, the system's principal office, and the Federal Information Processing Standards Publication 199 potential impact level.[33]

Number	System Name	Principal Office	Impact Level
1	Education Security Tracking and Reporting System	OM	MODERATE
2	Education Central Automated Processing System	OCIO	MODERATE
3	Common Origination and Disbursement	FSA	MODERATE
4	Person Authentication Service	FSA	MODERATE
5	Case and Activity Management System	OCR	MODERATE
6	Ombudsman Case Tracking System (cloud system)	FSA	MODERATE

As part of our original judgmental system sample, we selected the Presidential Scholars Program Electronic Application. However, we were informed that this system was in the process of being retired and was scheduled to be replaced in 2017. Therefore, we removed the system from our judgmental sample and replaced it with CAMS. These systems helped us ascertain the security control aspects relating to Configuration Management, Risk Management, and Contingency Planning.[34] In addition, these systems were the focus of our Web application vulnerability assessment and testing.

As of April 2016, the Department identified an inventory of 143 FISMA-reportable IT systems.

[32] High value assets are information resources, mission/business processes, and/or critical programs that are of particular interest to potential or actual adversaries. These assets may contain sensitive information used in critical Federal operations, or house unique collections of data (by size or content) making them of particular interest to criminal, politically-motivated, or state-sponsored adversaries for either direct exploitation of the data, to cause disruption to the delivery of critical services, or to cause a loss of confidence in the U.S. Government.

[33] 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.

[34] 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.

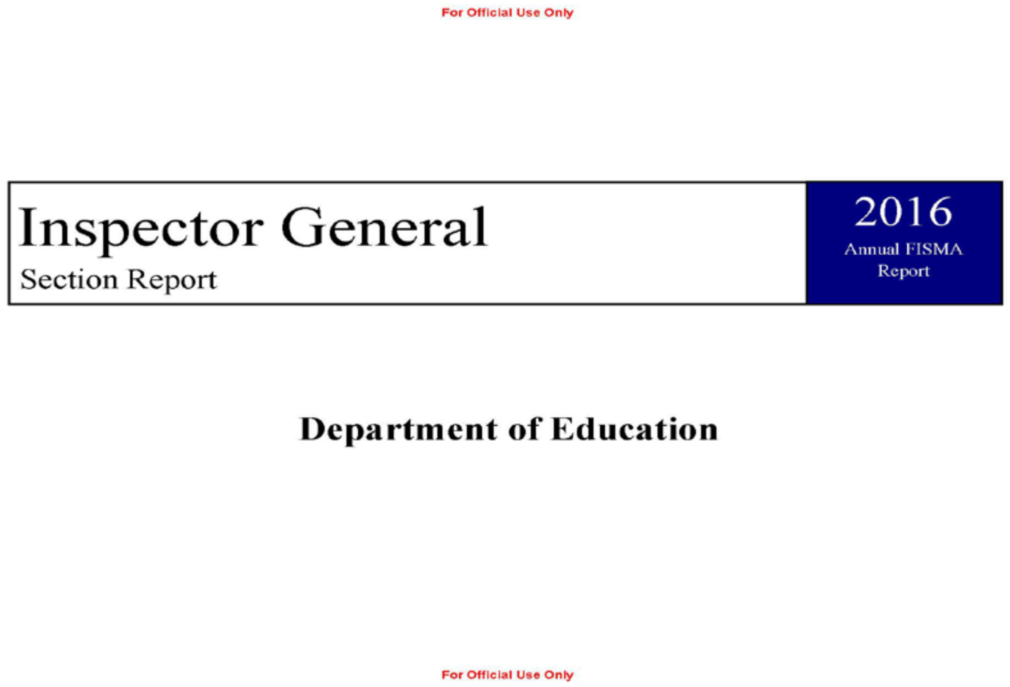
In addition to the sample of six systems, we also used sampling to test certain aspects in the areas of configuration management, identity and access management, and security training. For configuration management, we tested a sample of assets to validate the Department's asset decommissioning process. We judgmentally selected 17 out of 215 warehoused assets listed in the April and May 2016 Sanitization Reports.[35] We selected assets so that we included at least one from each equipment classification. For identity and access management, we confirmed the presence of appropriate access and training documentation for a sample of new hires. We requested from the Department a list of all new hires from October 1, 2015, through April 7, 2016. Of the 238 new hires that the Department identified, we selected a random sample of 25 and requested for each individual (1) signed and approved access agreements,; (2) documentation showing security awareness training was completed; and (3) documentation showing an Access Request/Termination Form was completed. Finally, for security training, we reviewed documentation of completed training for a sample of employees and contractors. We requested all Federal and contractor employees that completed cyber security and privacy training as of April 4, 2016. The Department identified 8,751 employees (4,190 Federal employees and 4,561 contractors). We randomly selected 78 federal employees and 78 contractors for a total sample size of 156. For each selected employee or contractor, we requested and reviewed security training completion certificates. Because we used either judgmental selections or auditor judgment to determine size for random samples, we did not project the results from the three samples.

For this audit, we reviewed the security controls and configuration settings for Web applications and at the Dell Services Federal Government data center that contains the application infrastructure for CAMS, EDCAPS, EDSTAR, and PAS; as well as the Total System Services, Inc., data center that contains the application infrastructure for COD. We used computer-processed data for the Configuration Management, Identity and Access Management, Security Training, and Remote Access Management metrics to support the findings summarized in this report. We also performed an assessment of the computer-processed data and determined these data were reliable for the purpose of our audit. To determine the extent of testing required for the assessment of the data's reliability, we assessed the importance of the data and corroborated it with other types of available evidence. The computer-processed data was verified to source and tested for accuracy according to relevant system controls until enough information was available to make a reliability determination. We conducted our fieldwork from February 2016 through September 2016, primarily at Department offices in Washington, D.C., and contractor facilities in Plano, Texas, and Columbus, Georgia. We conducted an exit conference with Department and FSA officials on October 26, 2016.

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.

[35] Equipment classification included a cross-cut representation of copiers, desktop personal computers, laptop personal computers, fax machines, printers, and scanners.

Enclosure 1: CyberScope FISMA Reporting Metrics



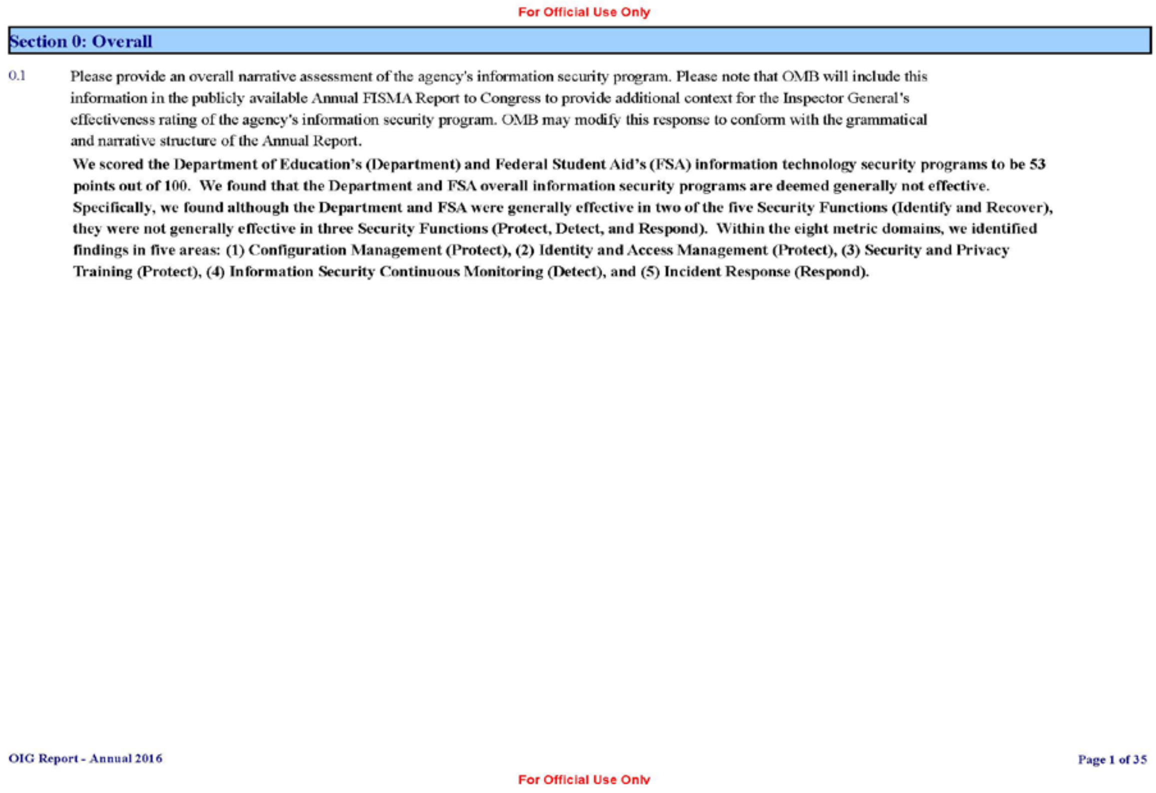
For Official Use Only

Inspector General
Section Report

2016
Annual FISMA
Report

Department of Education

For Official Use Only



For Official Use Only

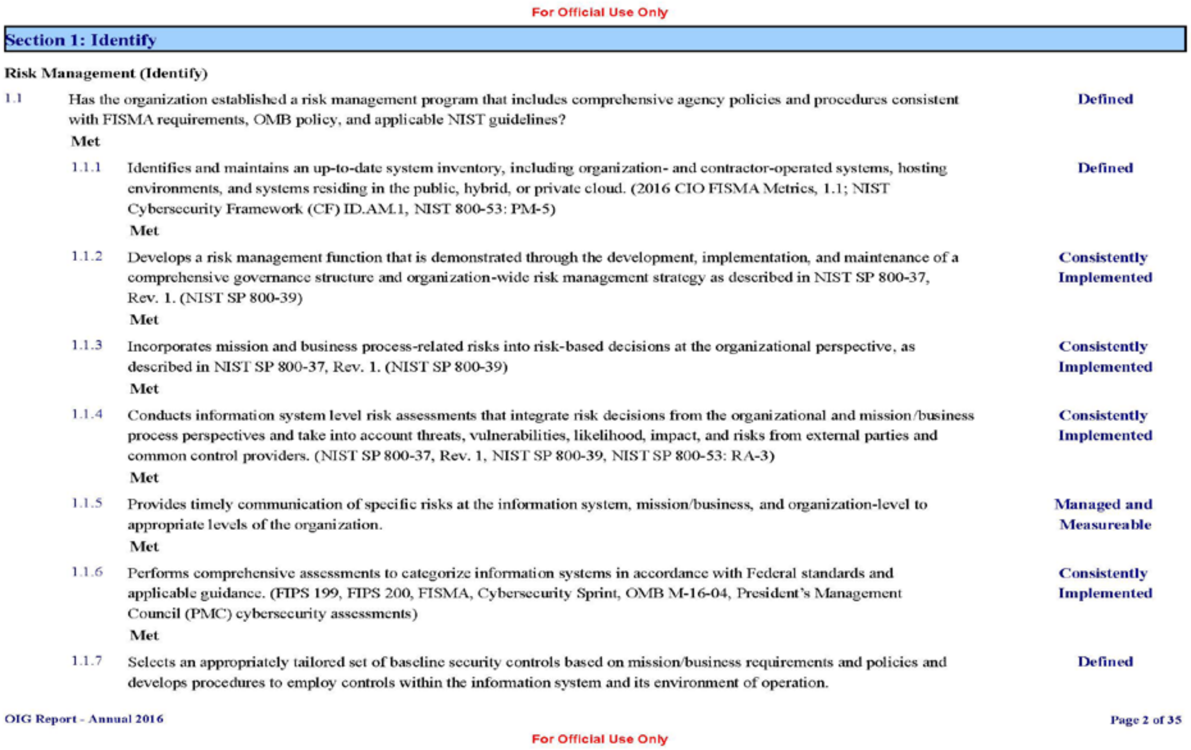
Section 0: Overall

0.1 Please provide an overall narrative assessment of the agency's information security program. 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 this response to conform with the grammatical and narrative structure of the Annual Report.

We scored the Department of Education's (Department) and Federal Student Aid's (FSA) information technology security programs to be 53 points out of 100. We found that the Department and FSA overall information security programs are deemed generally not effective. Specifically, we found although the Department and FSA were generally effective in two of the five Security Functions (Identify and Recover), they were not generally effective in three Security Functions (Protect, Detect, and Respond). Within the eight metric domains, we identified findings in five areas: (1) Configuration Management (Protect), (2) Identity and Access Management (Protect), (3) Security and Privacy Training (Protect), (4) Information Security Continuous Monitoring (Detect), and (5) Incident Response (Respond).

OIG Report - Annual 2016 Page 1 of 35

For Official Use Only



Section 1: Identify

Risk Management (Identify)

1.1 Has the organization established a risk management program that includes comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? — **Defined**

Met

1.1.1 Identifies and maintains an up-to-date system inventory, including organization- and contractor-operated systems, hosting environments, and systems residing in the public, hybrid, or private cloud. (2016 CIO FISMA Metrics, 1.1; NIST Cybersecurity Framework (CF) ID.AM.1, NIST 800-53: PM-5) — **Defined**

Met

1.1.2 Develops a risk management function that is demonstrated through the development, implementation, and maintenance of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1. (NIST SP 800-39) — **Consistently Implemented**

Met

1.1.3 Incorporates mission and business process-related risks into risk-based decisions at the organizational perspective, as described in NIST SP 800-37, Rev. 1. (NIST SP 800-39) — **Consistently Implemented**

Met

1.1.4 Conducts information system level risk assessments that integrate risk decisions from the organizational and mission/business process perspectives and take into account threats, vulnerabilities, likelihood, impact, and risks from external parties and common control providers. (NIST SP 800-37, Rev. 1, NIST SP 800-39, NIST SP 800-53: RA-3) — **Consistently Implemented**

Met

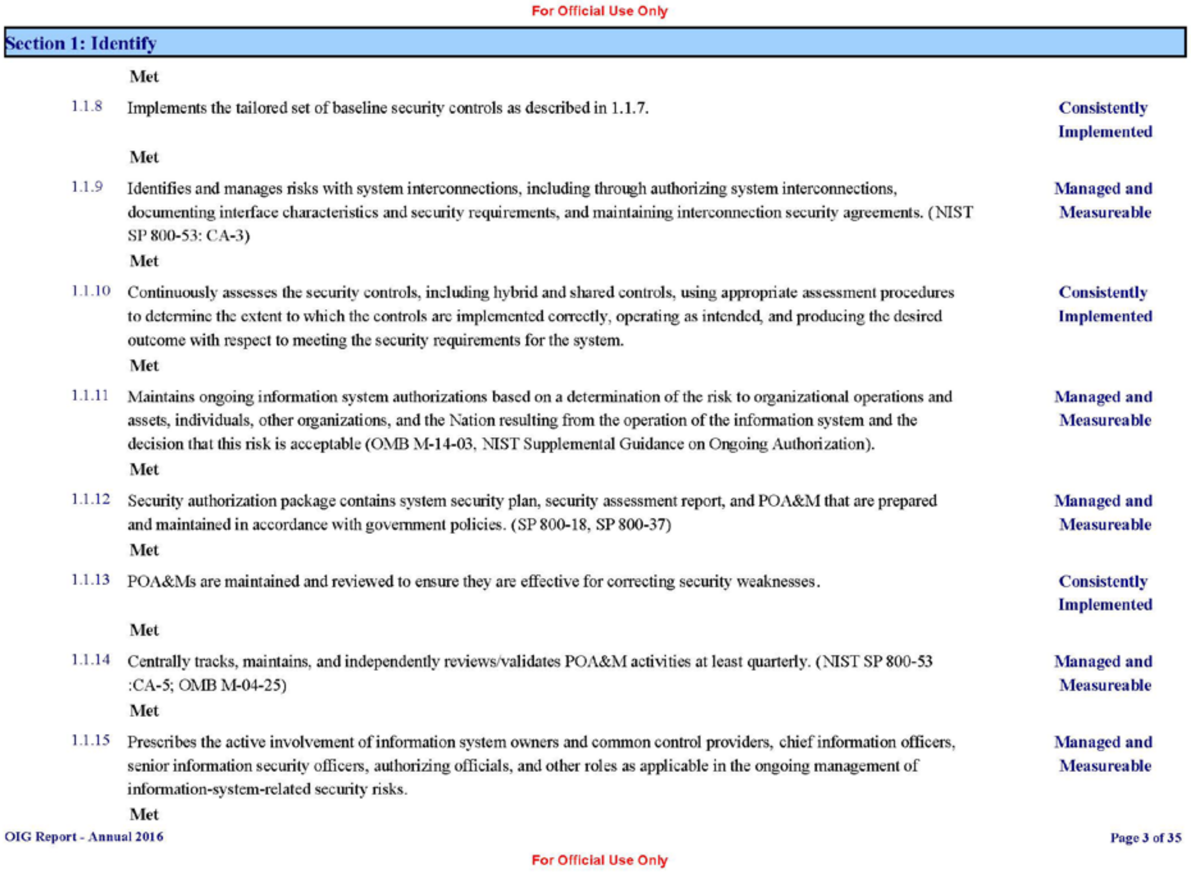
1.1.5 Provides timely communication of specific risks at the information system, mission/business, and organization-level to appropriate levels of the organization. — **Managed and Measureable**

Met

1.1.6 Performs comprehensive assessments to categorize information systems in accordance with Federal standards and applicable guidance. (FIPS 199, FIPS 200, FISMA, Cybersecurity Sprint, OMB M-16-04, President's Management Council (PMC) cybersecurity assessments) — **Consistently Implemented**

Met

1.1.7 Selects an appropriately tailored set of baseline security controls based on mission/business requirements and policies and develops procedures to employ controls within the information system and its environment of operation. — **Defined**



Section 1: Identify

Met

1.1.8 Implements the tailored set of baseline security controls as described in 1.1.7. — **Consistently Implemented**

Met

1.1.9 Identifies and manages risks with system interconnections, including through authorizing system interconnections, documenting interface characteristics and security requirements, and maintaining interconnection security agreements. (NIST SP 800-53: CA-3) — **Managed and Measureable**

Met

1.1.10 Continuously assesses the security controls, including hybrid and shared controls, using appropriate assessment procedures to determine 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 system. — **Consistently Implemented**

Met

1.1.11 Maintains ongoing information system authorizations based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable (OMB M-14-03, NIST Supplemental Guidance on Ongoing Authorization). — **Managed and Measureable**

Met

1.1.12 Security authorization package contains system security plan, security assessment report, and POA&M that are prepared and maintained in accordance with government policies. (SP 800-18, SP 800-37) — **Managed and Measureable**

Met

1.1.13 POA&Ms are maintained and reviewed to ensure they are effective for correcting security weaknesses. — **Consistently Implemented**

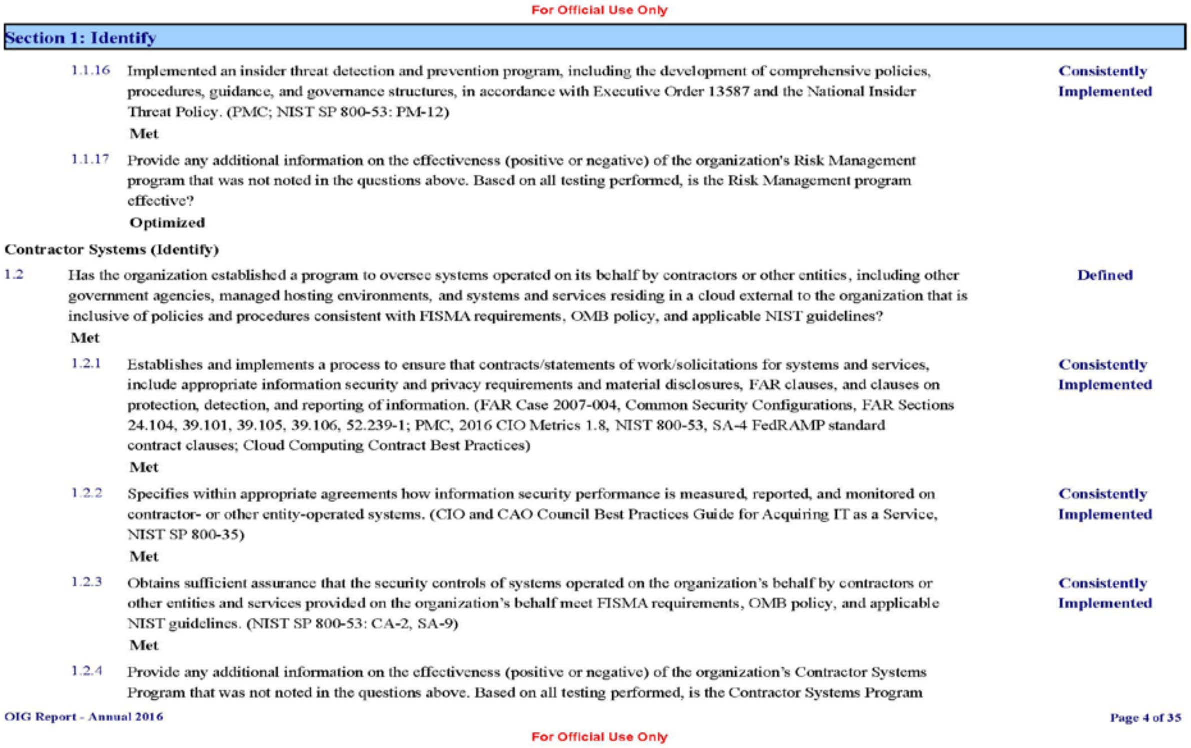
Met

1.1.14 Centrally tracks, maintains, and independently reviews/validates POA&M activities at least quarterly. (NIST SP 800-53 :CA-5; OMB M-04-25) — **Managed and Measureable**

Met

1.1.15 Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information-system-related security risks. — **Managed and Measureable**

Met



Section 1: Identify

1.1.16 Implemented an insider threat detection and prevention program, including the development of comprehensive policies, procedures, guidance, and governance structures, in accordance with Executive Order 13587 and the National Insider Threat Policy. (PMC; NIST SP 800-53: PM-12)

Met

Consistently Implemented

1.1.17 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. Based on all testing performed, is the Risk Management program effective?

Optimized

Contractor Systems (Identify)

1.2 Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including other government agencies, managed hosting environments, and systems and services residing in a cloud external to the organization that is inclusive of policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?

Met

Defined

1.2.1 Establishes and implements a process to ensure that contracts/statements of work/solicitations for systems and services, include appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information. (FAR Case 2007-004, Common Security Configurations, FAR Sections 24.104, 39.101, 39.105, 39.106, 52.239-1; PMC, 2016 CIO Metrics 1.8, NIST 800-53, SA-4 FedRAMP standard contract clauses; Cloud Computing Contract Best Practices)

Met

Consistently Implemented

1.2.2 Specifies within appropriate agreements how information security performance is measured, reported, and monitored on contractor- or other entity-operated systems. (CIO and CAO Council Best Practices Guide for Acquiring IT as a Service, NIST SP 800-35)

Met

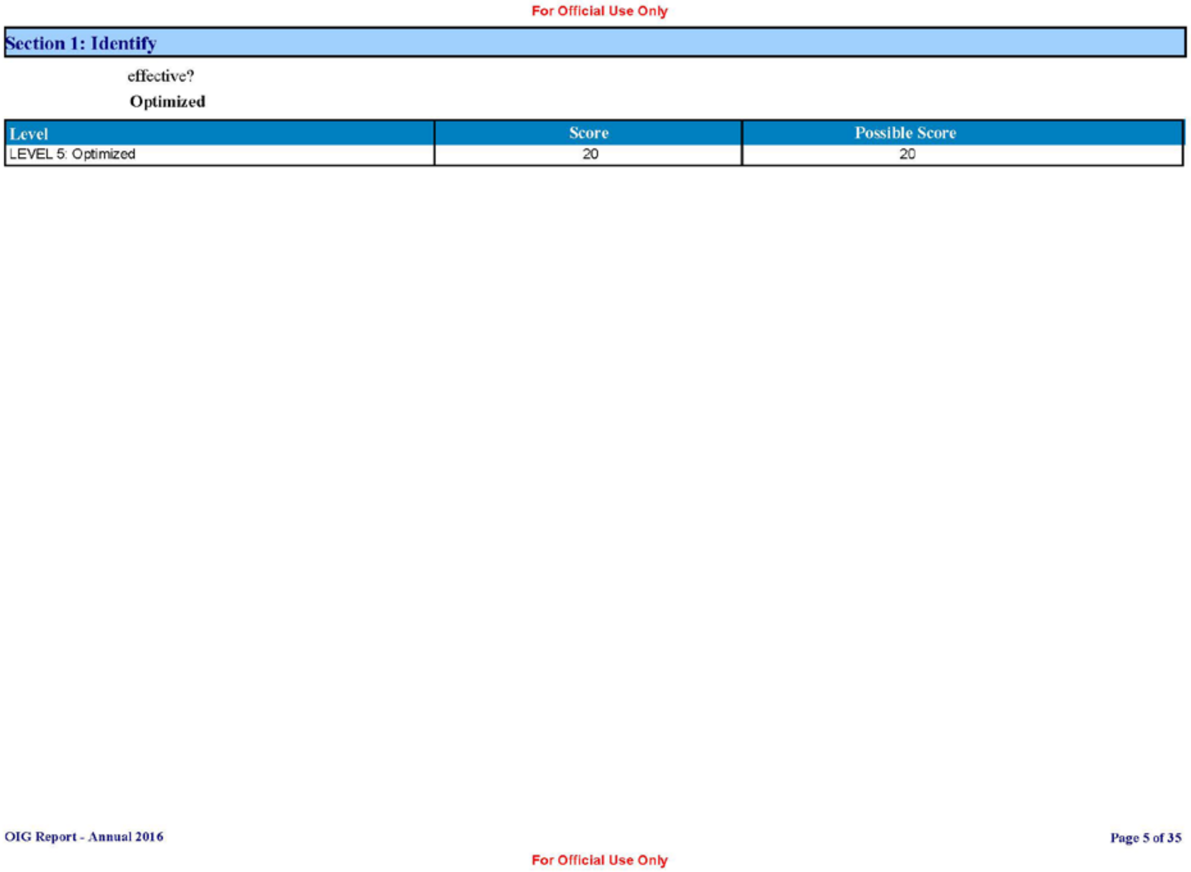
Consistently Implemented

1.2.3 Obtains sufficient assurance that the security controls of systems operated on the organization's behalf by contractors or other entities and services provided on the organization's behalf meet FISMA requirements, OMB policy, and applicable NIST guidelines. (NIST SP 800-53: CA-2, SA-9)

Met

Consistently Implemented

1.2.4 Provide any additional information on the effectiveness (positive or negative) of the organization's Contractor Systems Program that was not noted in the questions above. Based on all testing performed, is the Contractor Systems Program

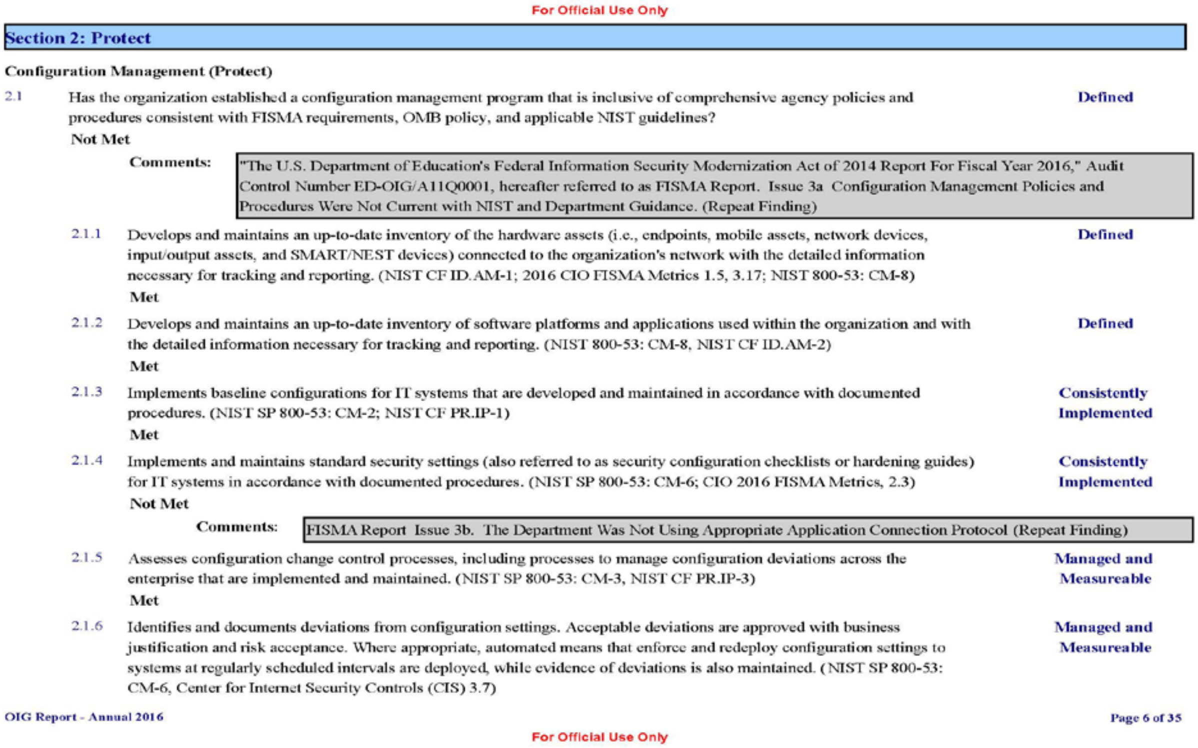


Section 1: Identify

effective?

Optimized

Level	Score	Possible Score
LEVEL 5: Optimized	20	20



For Official Use Only

Section 2: Protect

Configuration Management (Protect)

2.1 Has the organization established a configuration management program that is inclusive of comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Defined**

Not Met

Comments: "The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report For Fiscal Year 2016," Audit Control Number ED-OIG/A11Q0001, hereafter referred to as FISMA Report. Issue 3a Configuration Management Policies and Procedures Were Not Current with NIST and Department Guidance. (Repeat Finding)

2.1.1 Develops and maintains an up-to-date inventory of the hardware assets (i.e., endpoints, mobile assets, network devices, input/output assets, and SMART/NEST devices) connected to the organization's network with the detailed information necessary for tracking and reporting. (NIST CF ID.AM-1; 2016 CIO FISMA Metrics 1.5, 3.17; NIST 800-53: CM-8) **Defined**

Met

2.1.2 Develops and maintains an up-to-date inventory of software platforms and applications used within the organization and with the detailed information necessary for tracking and reporting. (NIST 800-53: CM-8, NIST CF ID.AM-2) **Defined**

Met

2.1.3 Implements baseline configurations for IT systems that are developed and maintained in accordance with documented procedures. (NIST SP 800-53: CM-2; NIST CF PR.IP-1) **Consistently Implemented**

Met

2.1.4 Implements and maintains standard security settings (also referred to as security configuration checklists or hardening guides) for IT systems in accordance with documented procedures. (NIST SP 800-53: CM-6; CIO 2016 FISMA Metrics, 2.3) **Consistently Implemented**

Not Met

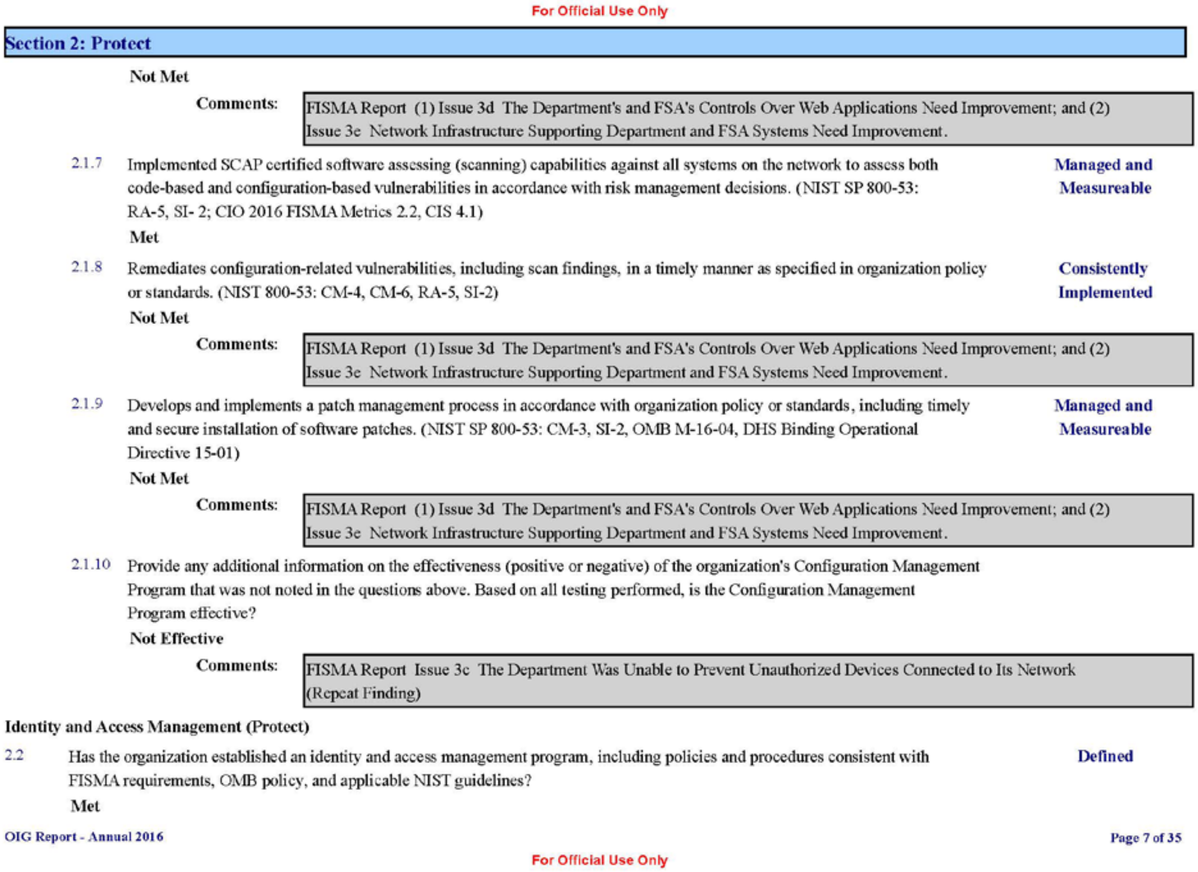
Comments: FISMA Report Issue 3b. The Department Was Not Using Appropriate Application Connection Protocol (Repeat Finding)

2.1.5 Assesses configuration change control processes, including processes to manage configuration deviations across the enterprise that are implemented and maintained. (NIST SP 800-53: CM-3, NIST CF PR.IP-3) **Managed and Measureable**

Met

2.1.6 Identifies and documents deviations from configuration settings. Acceptable deviations are approved with business justification and risk acceptance. Where appropriate, automated means that enforce and redeploy configuration settings to systems at regularly scheduled intervals are deployed, while evidence of deviations is also maintained. (NIST SP 800-53: CM-6, Center for Internet Security Controls (CIS) 3.7) **Managed and Measureable**

For Official Use Only



For Official Use Only

Section 2: Protect

Not Met

Comments: FISMA Report (1) Issue 3d The Department's and FSA's Controls Over Web Applications Need Improvement; and (2) Issue 3e Network Infrastructure Supporting Department and FSA Systems Need Improvement.

2.1.7 Implemented SCAP certified software assessing (scanning) capabilities against all systems on the network to assess both code-based and configuration-based vulnerabilities in accordance with risk management decisions. (NIST SP 800-53: RA-5, SI- 2; CIO 2016 FISMA Metrics 2.2, CIS 4.1) **Managed and Measureable**

Met

2.1.8 Remediates configuration-related vulnerabilities, including scan findings, in a timely manner as specified in organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2) **Consistently Implemented**

Not Met

Comments: FISMA Report (1) Issue 3d The Department's and FSA's Controls Over Web Applications Need Improvement; and (2) Issue 3e Network Infrastructure Supporting Department and FSA Systems Need Improvement.

2.1.9 Develops and implements a patch management process in accordance with organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3, SI-2, OMB M-16-04, DHS Binding Operational Directive 15-01) **Managed and Measureable**

Not Met

Comments: FISMA Report (1) Issue 3d The Department's and FSA's Controls Over Web Applications Need Improvement; and (2) Issue 3e Network Infrastructure Supporting Department and FSA Systems Need Improvement.

2.1.10 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. Based on all testing performed, is the Configuration Management Program effective?

Not Effective

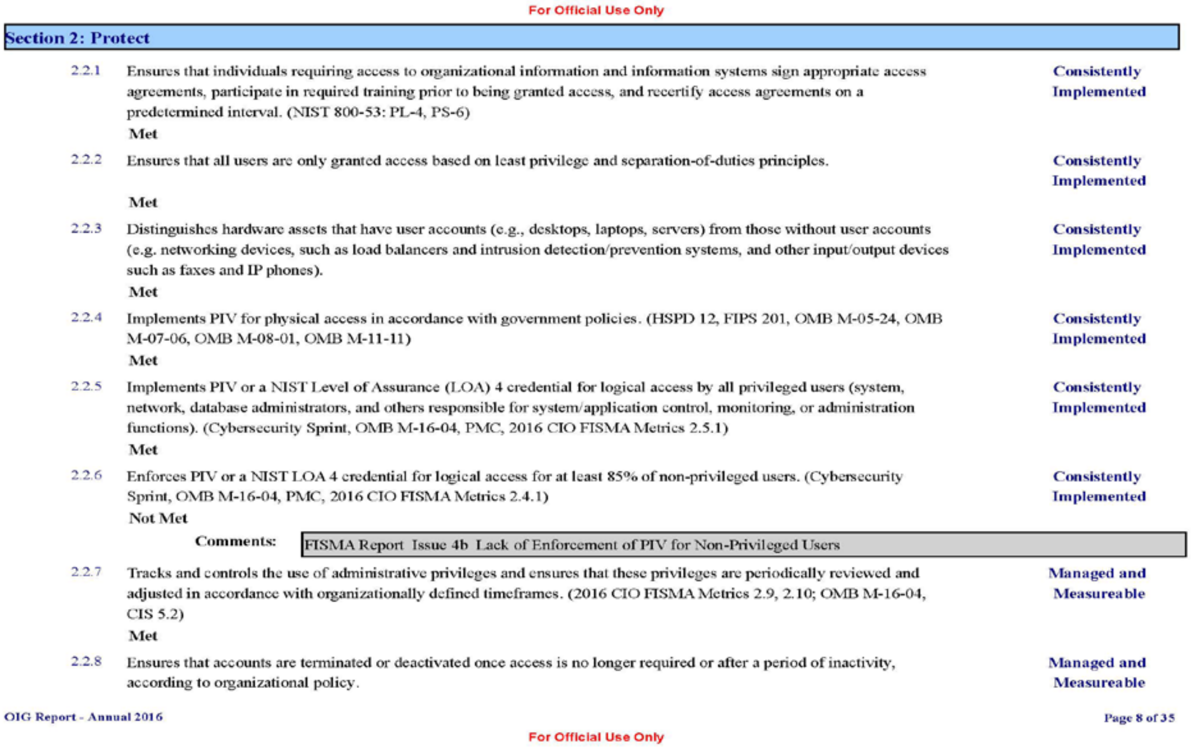
Comments: FISMA Report Issue 3c The Department Was Unable to Prevent Unauthorized Devices Connected to Its Network (Repeat Finding)

Identity and Access Management (Protect)

2.2 Has the organization established an identity and access management program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Defined**

Met

For Official Use Only



Section 2: Protect

2.2.1 Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements, participate in required training prior to being granted access, and recertify access agreements on a predetermined interval. (NIST 800-53: PL-4, PS-6) — **Consistently Implemented**

Met

2.2.2 Ensures that all users are only granted access based on least privilege and separation-of-duties principles. — **Consistently Implemented**

Met

2.2.3 Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. networking devices, such as load balancers and intrusion detection/prevention systems, and other input/output devices such as faxes and IP phones). — **Consistently Implemented**

Met

2.2.4 Implements PIV for physical access in accordance with government policies. (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11) — **Consistently Implemented**

Met

2.2.5 Implements PIV or a NIST Level of Assurance (LOA) 4 credential for logical access by all privileged users (system, network, database administrators, and others responsible for system/application control, monitoring, or administration functions). (Cybersecurity Sprint, OMB M-16-04, PMC, 2016 CIO FISMA Metrics 2.5.1) — **Consistently Implemented**

Met

2.2.6 Enforces PIV or a NIST LOA 4 credential for logical access for at least 85% of non-privileged users. (Cybersecurity Sprint, OMB M-16-04, PMC, 2016 CIO FISMA Metrics 2.4.1) — **Consistently Implemented**

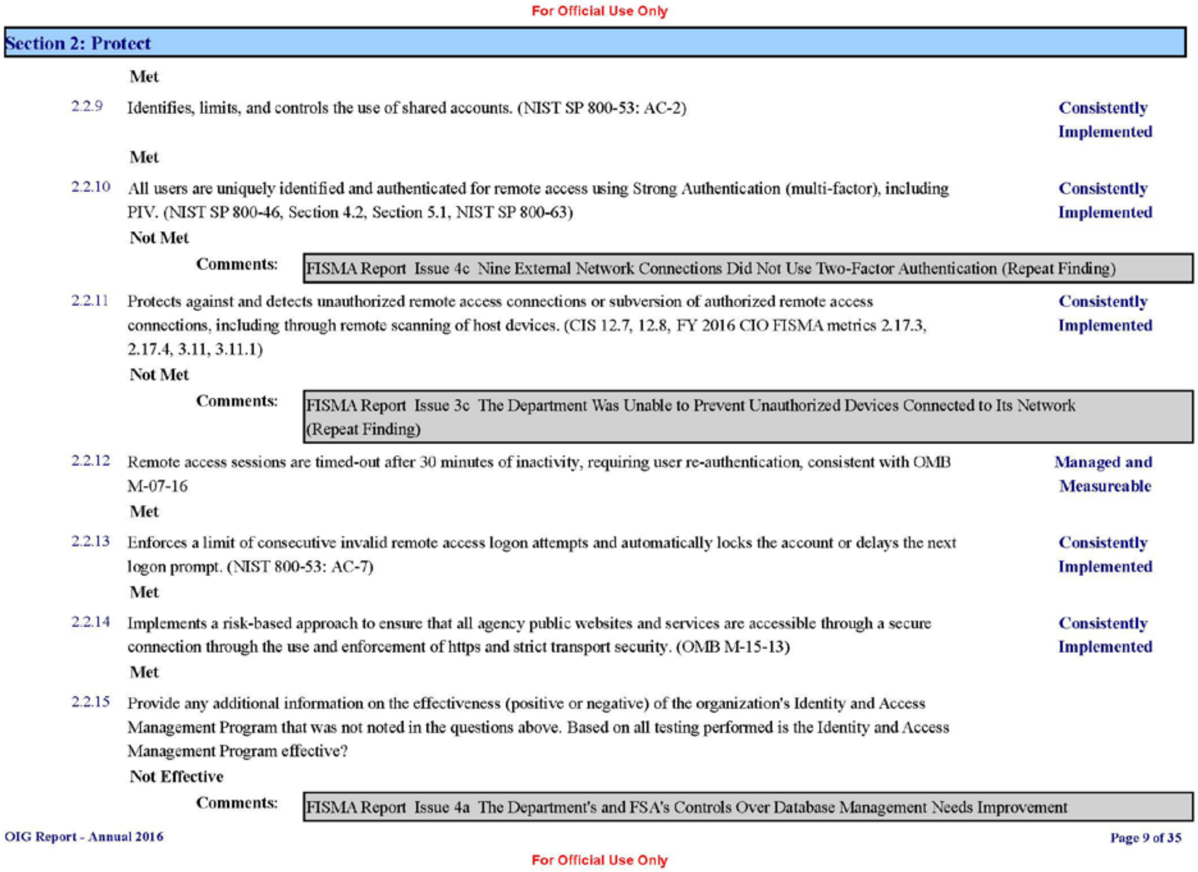
Not Met

Comments: FISMA Report Issue 4b Lack of Enforcement of PIV for Non-Privileged Users

2.2.7 Tracks and controls the use of administrative privileges and ensures that these privileges are periodically reviewed and adjusted in accordance with organizationally defined timeframes. (2016 CIO FISMA Metrics 2.9, 2.10; OMB M-16-04, CIS 5.2) — **Managed and Measureable**

Met

2.2.8 Ensures that accounts are terminated or deactivated once access is no longer required or after a period of inactivity, according to organizational policy. — **Managed and Measureable**



Section 2: Protect

Met

2.2.9 Identifies, limits, and controls the use of shared accounts. (NIST SP 800-53: AC-2) — **Consistently Implemented**

Met

2.2.10 All users are uniquely identified and authenticated for remote access using Strong Authentication (multi-factor), including PIV. (NIST SP 800-46, Section 4.2, Section 5.1, NIST SP 800-63) — **Consistently Implemented**

Not Met

Comments: FISMA Report Issue 4c Nine External Network Connections Did Not Use Two-Factor Authentication (Repeat Finding)

2.2.11 Protects against and detects unauthorized remote access connections or subversion of authorized remote access connections, including through remote scanning of host devices. (CIS 12.7, 12.8, FY 2016 CIO FISMA metrics 2.17.3, 2.17.4, 3.11, 3.11.1) — **Consistently Implemented**

Not Met

Comments: FISMA Report Issue 3c The Department Was Unable to Prevent Unauthorized Devices Connected to Its Network (Repeat Finding)

2.2.12 Remote access sessions are timed-out after 30 minutes of inactivity, requiring user re-authentication, consistent with OMB M-07-16 — **Managed and Measureable**

Met

2.2.13 Enforces a limit of consecutive invalid remote access logon attempts and automatically locks the account or delays the next logon prompt. (NIST 800-53: AC-7) — **Consistently Implemented**

Met

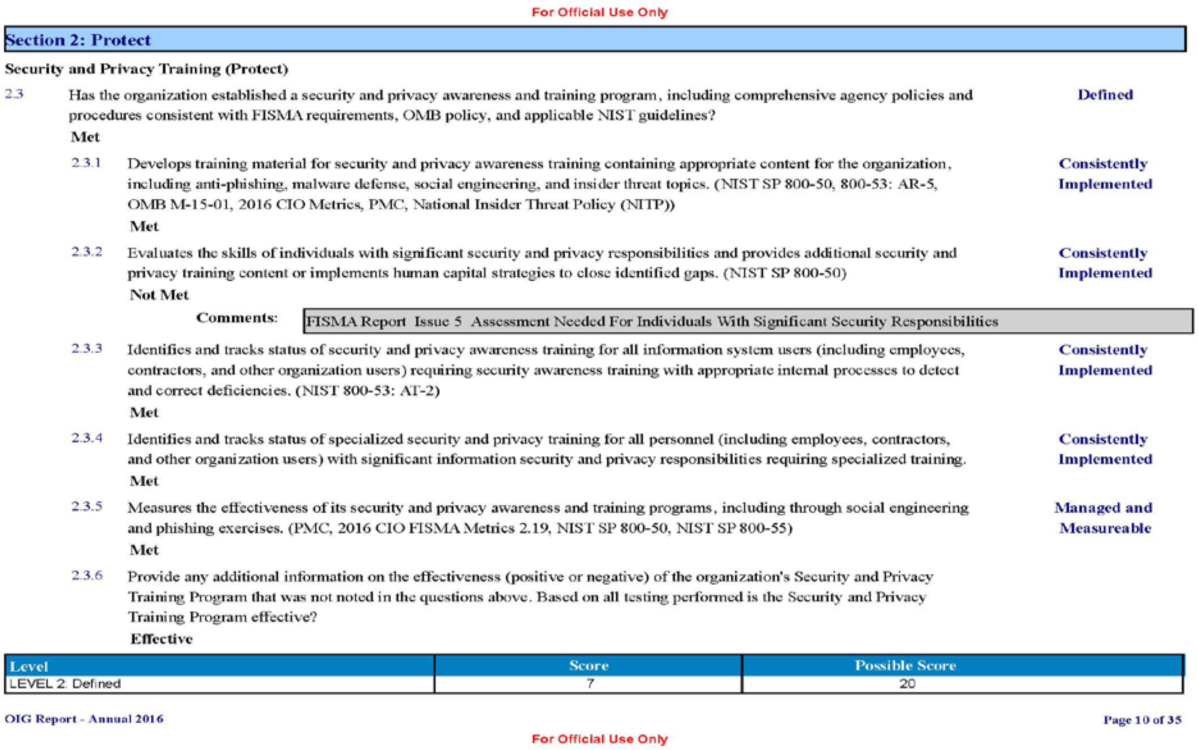
2.2.14 Implements a risk-based approach to ensure that all agency public websites and services are accessible through a secure connection through the use and enforcement of https and strict transport security. (OMB M-15-13) — **Consistently Implemented**

Met

2.2.15 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. Based on all testing performed is the Identity and Access Management Program effective?

Not Effective

Comments: FISMA Report Issue 4a The Department's and FSA's Controls Over Database Management Needs Improvement



For Official Use Only

Section 2: Protect

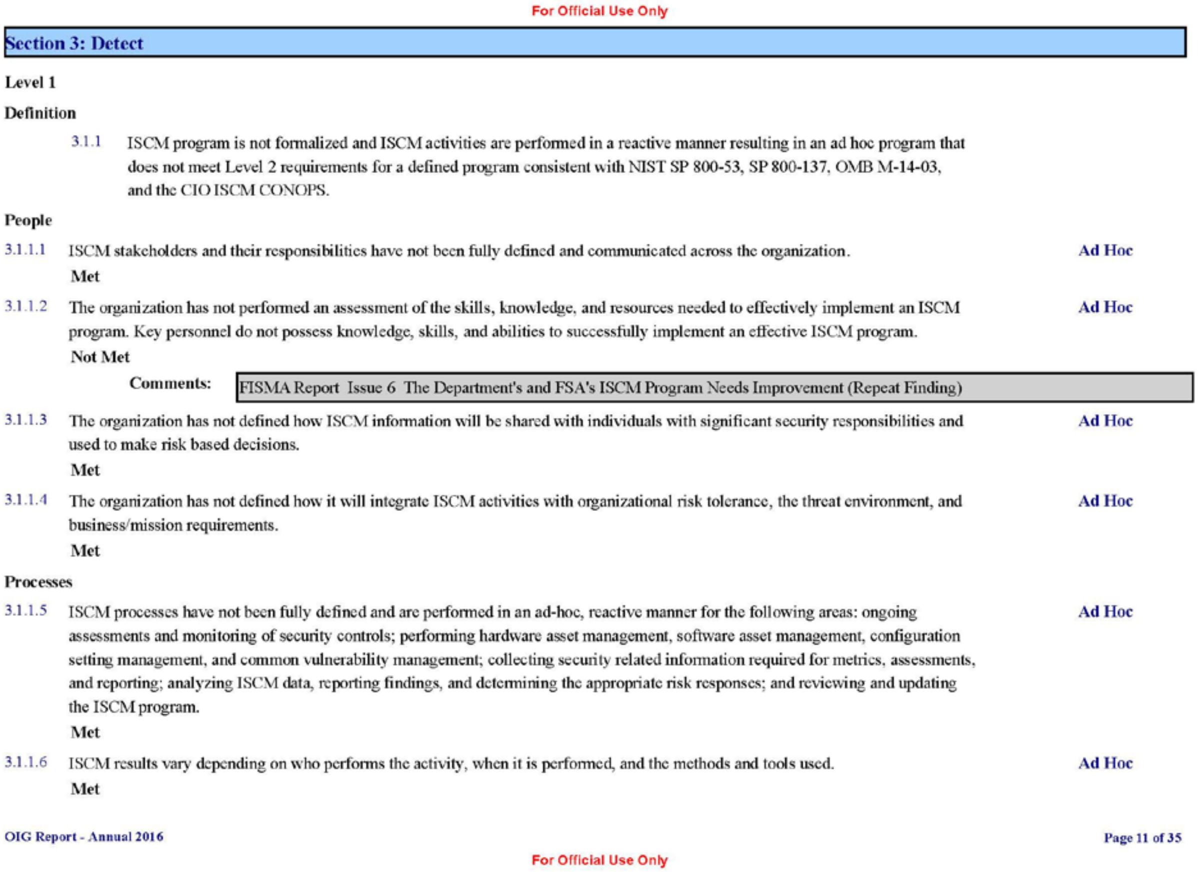
Security and Privacy Training (Protect)

2.3	Has the organization established a security and privacy awareness and training program, including comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Met**	Defined
2.3.1	Develops training material for security and privacy awareness training containing appropriate content for the organization, including anti-phishing, malware defense, social engineering, and insider threat topics. (NIST SP 800-50, 800-53: AR-5, OMB M-15-01, 2016 CIO Metrics, PMC, National Insider Threat Policy (NITP)) **Met**	Consistently Implemented
2.3.2	Evaluates the skills of individuals with significant security and privacy responsibilities and provides additional security and privacy training content or implements human capital strategies to close identified gaps. (NIST SP 800-50) **Not Met** **Comments:** FISMA Report Issue 5 Assessment Needed For Individuals With Significant Security Responsibilities	Consistently Implemented
2.3.3	Identifies and tracks status of security and privacy awareness training for all information system users (including employees, contractors, and other organization users) requiring security awareness training with appropriate internal processes to detect and correct deficiencies. (NIST 800-53: AT-2) **Met**	Consistently Implemented
2.3.4	Identifies and tracks status of specialized security and privacy training for all personnel (including employees, contractors, and other organization users) with significant information security and privacy responsibilities requiring specialized training. **Met**	Consistently Implemented
2.3.5	Measures the effectiveness of its security and privacy awareness and training programs, including through social engineering and phishing exercises. (PMC, 2016 CIO FISMA Metrics 2.19, NIST SP 800-50, NIST SP 800-55) **Met**	Managed and Measureable
2.3.6	Provide any additional information on the effectiveness (positive or negative) of the organization's Security and Privacy Training Program that was not noted in the questions above. Based on all testing performed is the Security and Privacy Training Program effective? **Effective**	

Level	Score	Possible Score
LEVEL 2: Defined	7	20

OIG Report - Annual 2016 Page 10 of 35

For Official Use Only



For Official Use Only

Section 3: Detect

Level 1

Definition

3.1.1 ISCM program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.

People

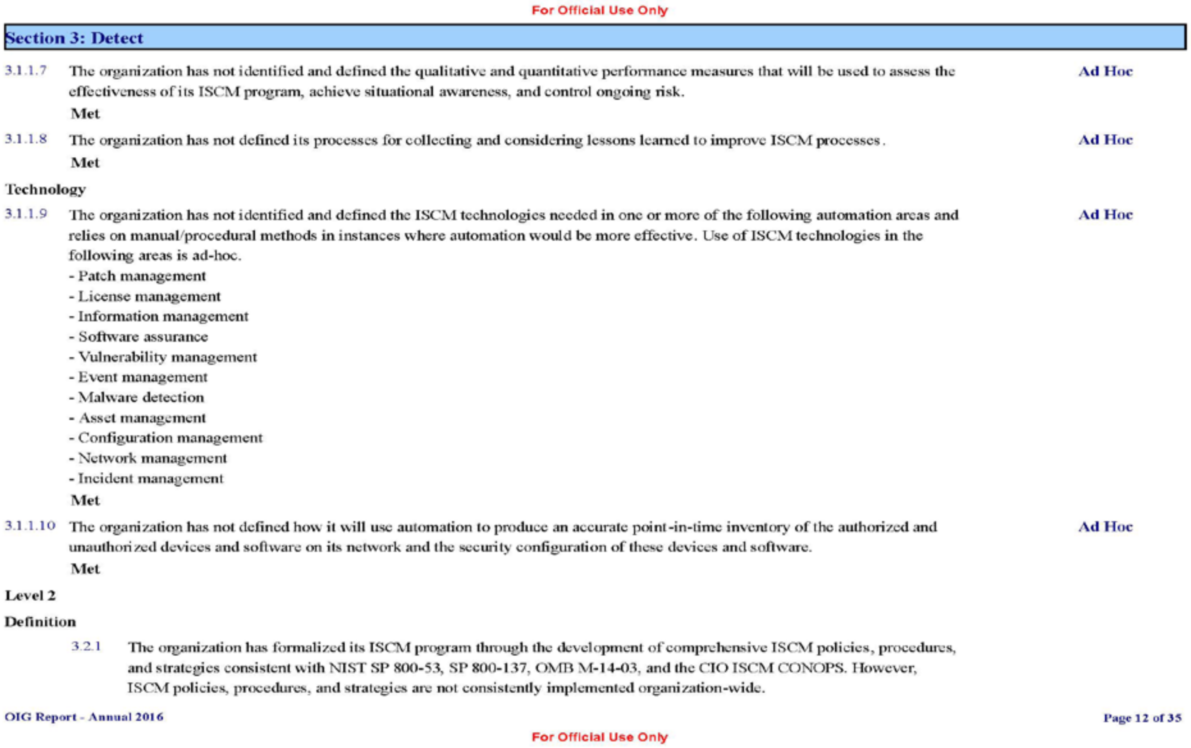
3.1.1.1	ISCM stakeholders and their responsibilities have not been fully defined and communicated across the organization. **Met**	Ad Hoc
3.1.1.2	The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. Key personnel do not possess knowledge, skills, and abilities to successfully implement an effective ISCM program. **Not Met** **Comments:** FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)	Ad Hoc
3.1.1.3	The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk based decisions. **Met**	Ad Hoc
3.1.1.4	The organization has not defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements. **Met**	Ad Hoc

Processes

3.1.1.5	ISCM processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. **Met**	Ad Hoc
3.1.1.6	ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. **Met**	Ad Hoc

OIG Report - Annual 2016 Page 11 of 35

For Official Use Only



For Official Use Only

Section 3: Detect

3.1.1.7 The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. **Ad Hoc**

Met

3.1.1.8 The organization has not defined its processes for collecting and considering lessons learned to improve ISCM processes. **Ad Hoc**

Met

Technology

3.1.1.9 The organization has not identified and defined the ISCM technologies needed in one or more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective. Use of ISCM technologies in the following areas is ad-hoc. **Ad Hoc**

- Patch management
- License management
- Information management
- Software assurance
- Vulnerability management
- Event management
- Malware detection
- Asset management
- Configuration management
- Network management
- Incident management

Met

3.1.1.10 The organization has not defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. **Ad Hoc**

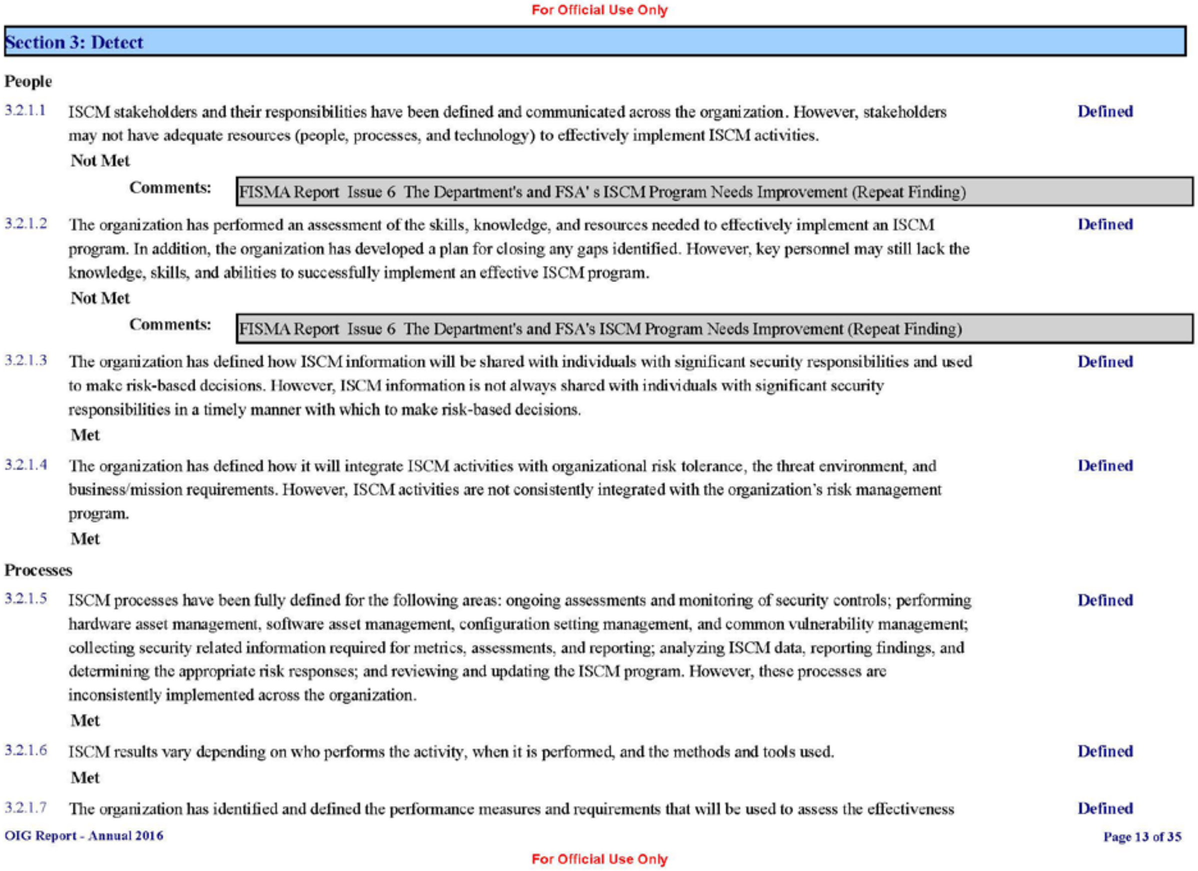
Met

Level 2

Definition

3.2.1 The organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. However, ISCM policies, procedures, and strategies are not consistently implemented organization-wide.

For Official Use Only



For Official Use Only

Section 3: Detect

People

3.2.1.1 ISCM stakeholders and their responsibilities have been defined and communicated across the organization. However, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement ISCM activities. **Defined**

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA' s ISCM Program Needs Improvement (Repeat Finding)

3.2.1.2 The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. In addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective ISCM program. **Defined**

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

3.2.1.3 The organization has defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions. However, ISCM information is not always shared with individuals with significant security responsibilities in a timely manner with which to make risk-based decisions. **Defined**

Met

3.2.1.4 The organization has defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements. However, ISCM activities are not consistently integrated with the organization's risk management program. **Defined**

Met

Processes

3.2.1.5 ISCM processes have been fully defined for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. However, these processes are inconsistently implemented across the organization. **Defined**

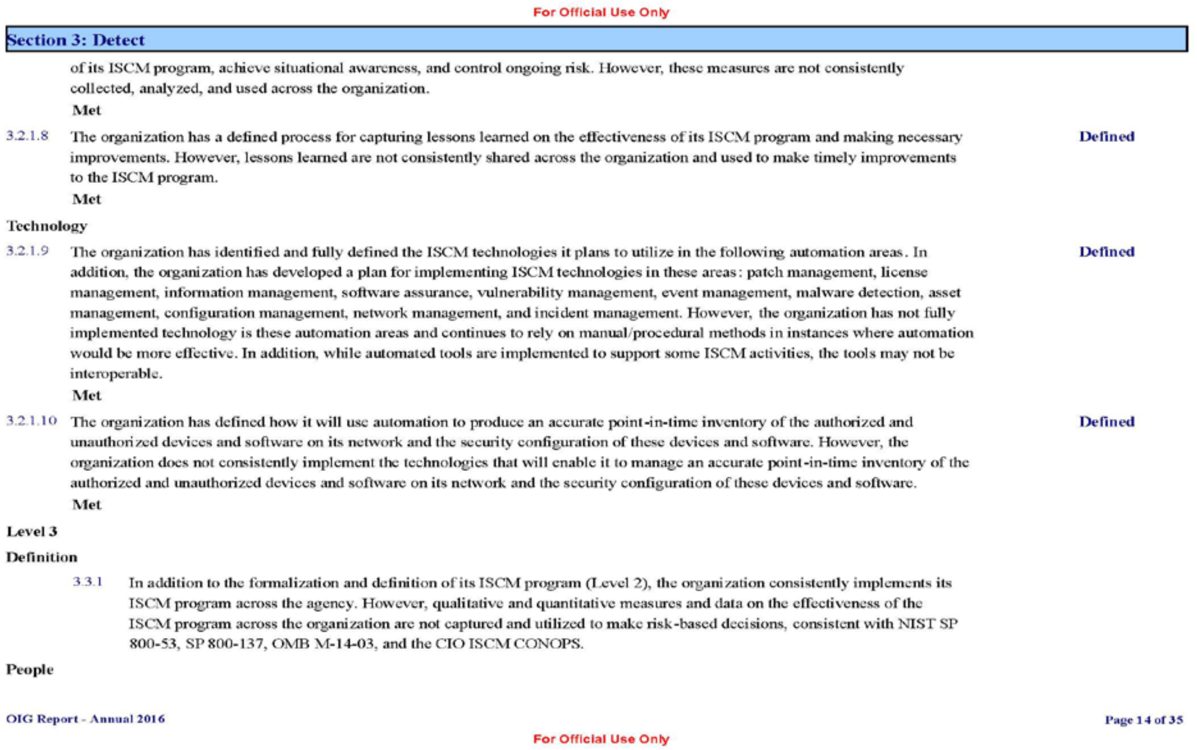
Met

3.2.1.6 ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. **Defined**

Met

3.2.1.7 The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness **Defined**

For Official Use Only



Section 3: Detect

of its ISCM program, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization.

Met

3.2.1.8 The organization has a defined process for capturing lessons learned on the effectiveness of its ISCM program and making necessary improvements. However, lessons learned are not consistently shared across the organization and used to make timely improvements to the ISCM program. **Defined**

Met

Technology

3.2.1.9 The organization has identified and fully defined the ISCM technologies it plans to utilize in the following automation areas. In addition, the organization has developed a plan for implementing ISCM technologies in these areas: patch management, license management, information management, software assurance, vulnerability management, event management, malware detection, asset management, configuration management, network management, and incident management. However, the organization has not fully implemented technology is these automation areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while automated tools are implemented to support some ISCM activities, the tools may not be interoperable. **Defined**

Met

3.2.1.10 The organization has defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. However, the organization does not consistently implement the technologies that will enable it to manage an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. **Defined**

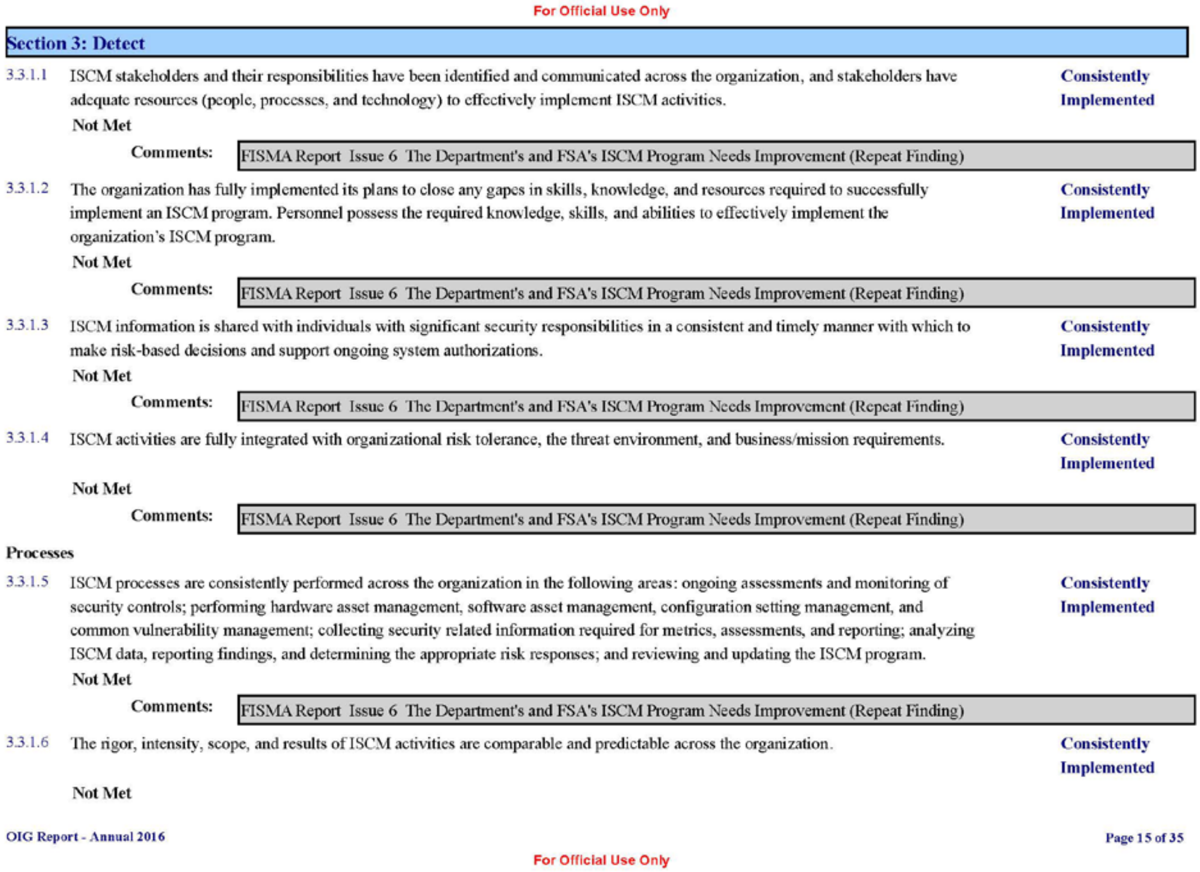
Met

Level 3

Definition

3.3.1 In addition to the formalization and definition of its ISCM program (Level 2), the organization consistently implements its ISCM program across the agency. However, qualitative and quantitative measures and data on the effectiveness of the ISCM program across the organization are not captured and utilized to make risk-based decisions, consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.

People



Section 3: Detect

3.3.1.1 ISCM stakeholders and their responsibilities have been identified and communicated across the organization, and stakeholders have adequate resources (people, processes, and technology) to effectively implement ISCM activities. **Consistently Implemented**

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

3.3.1.2 The organization has fully implemented its plans to close any gapes in skills, knowledge, and resources required to successfully implement an ISCM program. Personnel possess the required knowledge, skills, and abilities to effectively implement the organization's ISCM program. **Consistently Implemented**

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

3.3.1.3 ISCM information is shared with individuals with significant security responsibilities in a consistent and timely manner with which to make risk-based decisions and support ongoing system authorizations. **Consistently Implemented**

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

3.3.1.4 ISCM activities are fully integrated with organizational risk tolerance, the threat environment, and business/mission requirements. **Consistently Implemented**

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

Processes

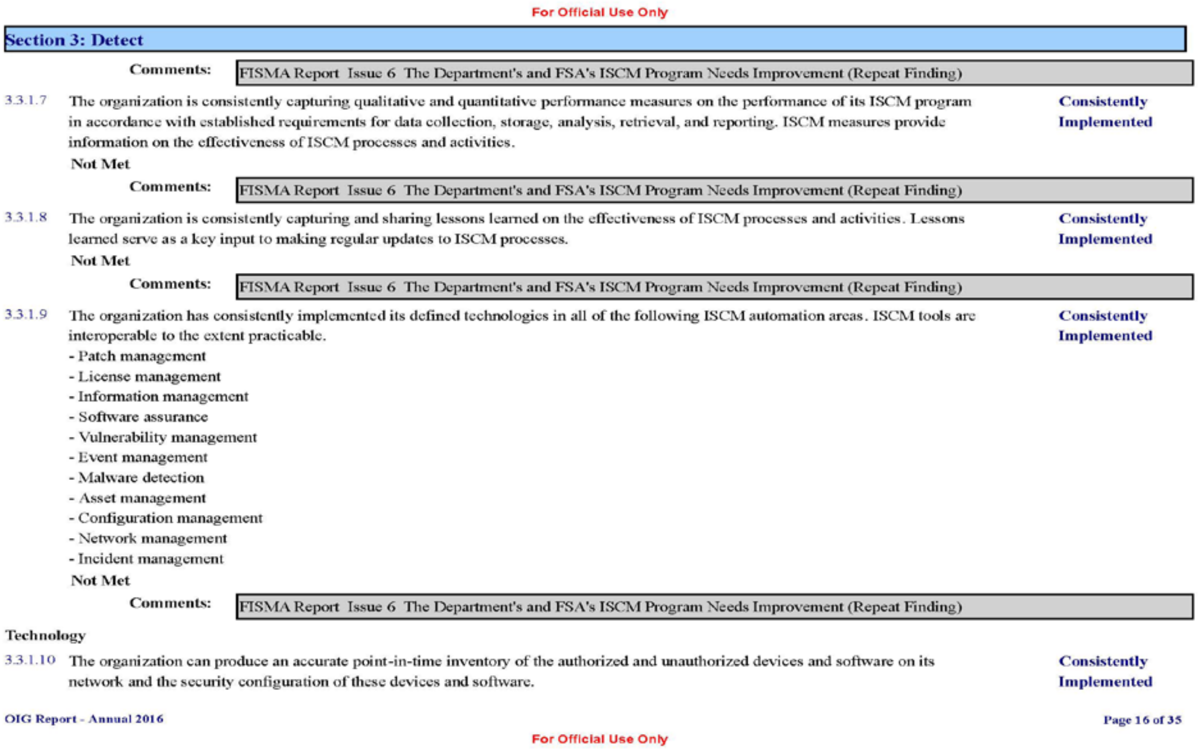
3.3.1.5 ISCM processes are consistently performed across the organization in the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. **Consistently Implemented**

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

3.3.1.6 The rigor, intensity, scope, and results of ISCM activities are comparable and predictable across the organization. **Consistently Implemented**

Not Met



Section 3: Detect

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

3.3.1.7 The organization is consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting. ISCM measures provide information on the effectiveness of ISCM processes and activities. **Consistently Implemented**

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

3.3.1.8 The organization is consistently capturing and sharing lessons learned on the effectiveness of ISCM processes and activities. Lessons learned serve as a key input to making regular updates to ISCM processes. **Consistently Implemented**

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

3.3.1.9 The organization has consistently implemented its defined technologies in all of the following ISCM automation areas. ISCM tools are interoperable to the extent practicable. **Consistently Implemented**

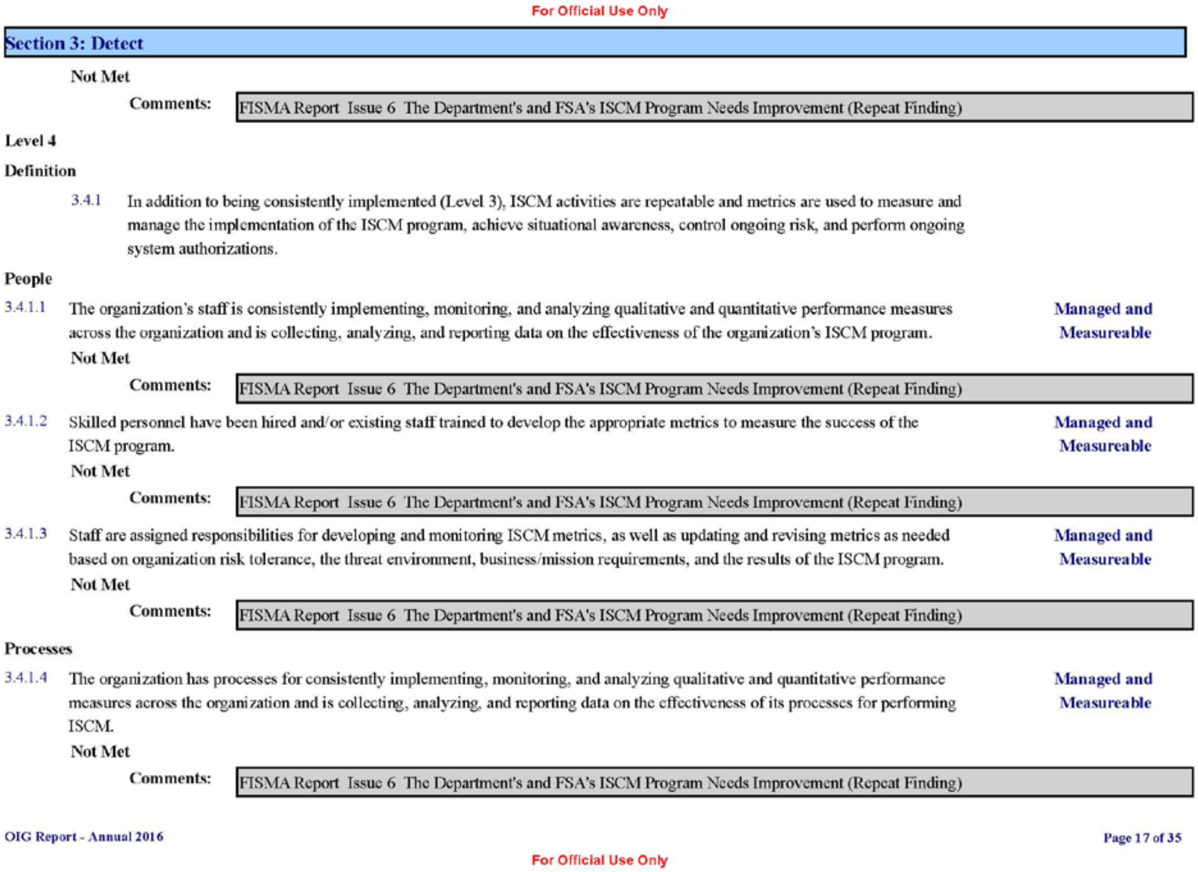
- Patch management
- License management
- Information management
- Software assurance
- Vulnerability management
- Event management
- Malware detection
- Asset management
- Configuration management
- Network management
- Incident management

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

Technology

3.3.1.10 The organization can produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. **Consistently Implemented**



Section 3: Detect

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

Level 4

Definition

3.4.1 In addition to being consistently implemented (Level 3), ISCM activities are repeatable and metrics are used to measure and manage the implementation of the ISCM program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.

People

3.4.1.1 The organization's staff is consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of the organization's ISCM program. **Managed and Measureable**

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

3.4.1.2 Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the ISCM program. **Managed and Measureable**

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

3.4.1.3 Staff are assigned responsibilities for developing and monitoring ISCM metrics, as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the ISCM program. **Managed and Measureable**

Not Met

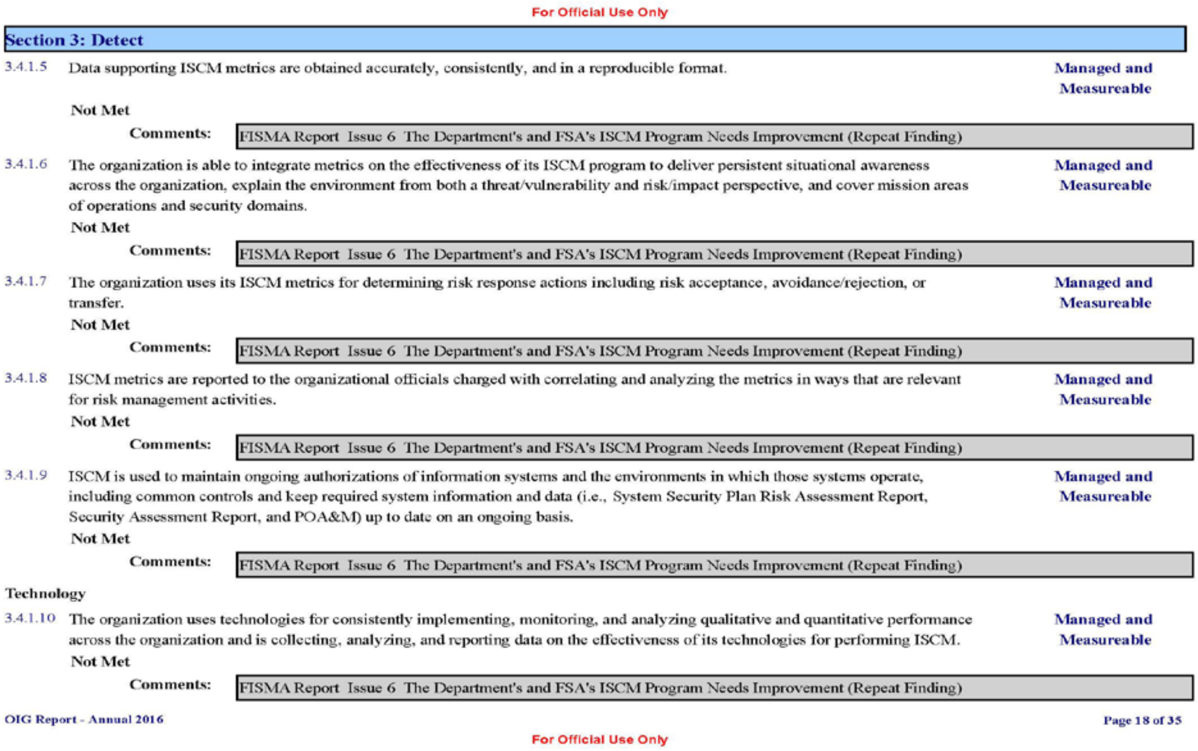
Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

Processes

3.4.1.4 The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing ISCM. **Managed and Measureable**

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)



Section 3: Detect

3.4.1.5 Data supporting ISCM metrics are obtained accurately, consistently, and in a reproducible format. — Managed and Measureable

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

3.4.1.6 The organization is able to integrate metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations and security domains. — Managed and Measureable

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

3.4.1.7 The organization uses its ISCM metrics for determining risk response actions including risk acceptance, avoidance/rejection, or transfer. — Managed and Measureable

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

3.4.1.8 ISCM metrics are reported to the organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities. — Managed and Measureable

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

3.4.1.9 ISCM is used to maintain ongoing authorizations of information systems and the environments in which those systems operate, including common controls and keep required system information and data (i.e., System Security Plan Risk Assessment Report, Security Assessment Report, and POA&M) up to date on an ongoing basis. — Managed and Measureable

Not Met

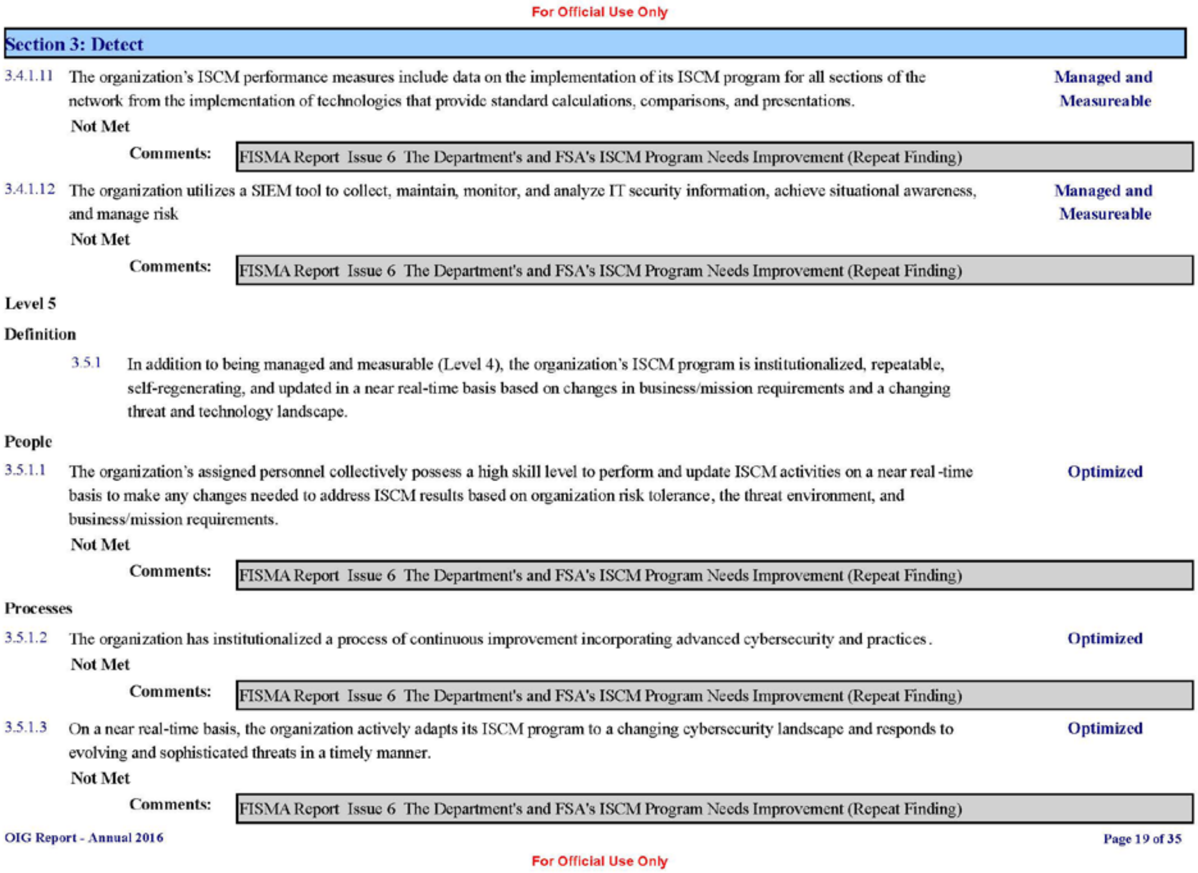
Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

Technology

3.4.1.10 The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing ISCM. — Managed and Measureable

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)



Section 3: Detect

3.4.1.11 The organization's ISCM performance measures include data on the implementation of its ISCM program for all sections of the network from the implementation of technologies that provide standard calculations, comparisons, and presentations. — Managed and Measureable

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

3.4.1.12 The organization utilizes a SIEM tool to collect, maintain, monitor, and analyze IT security information, achieve situational awareness, and manage risk — Managed and Measureable

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

Level 5

Definition

3.5.1 In addition to being managed and measurable (Level 4), the organization's ISCM program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape.

People

3.5.1.1 The organization's assigned personnel collectively possess a high skill level to perform and update ISCM activities on a near real-time basis to make any changes needed to address ISCM results based on organization risk tolerance, the threat environment, and business/mission requirements. — Optimized

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

Processes

3.5.1.2 The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity and practices. — Optimized

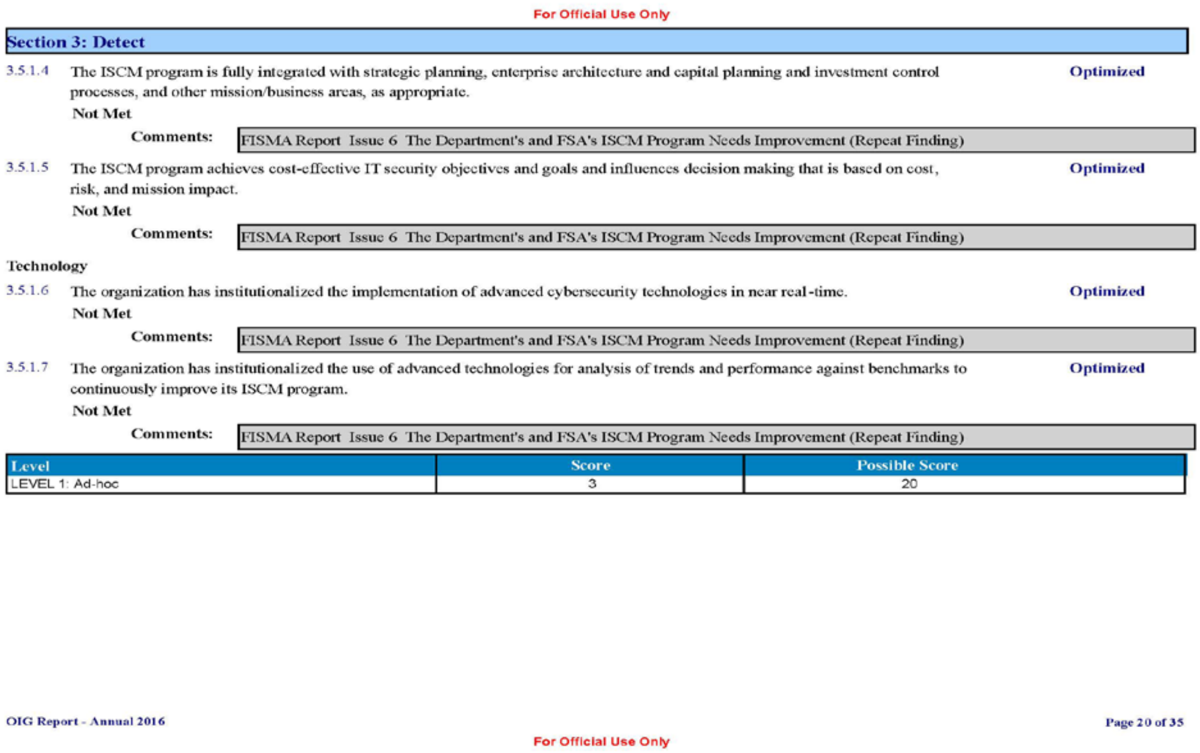
Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

3.5.1.3 On a near real-time basis, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. — Optimized

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)



For Official Use Only

Section 3: Detect

3.5.1.4 The ISCM program is fully integrated with strategic planning, enterprise architecture and capital planning and investment control processes, and other mission/business areas, as appropriate. **Optimized**

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

3.5.1.5 The ISCM program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact. **Optimized**

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

Technology

3.5.1.6 The organization has institutionalized the implementation of advanced cybersecurity technologies in near real-time. **Optimized**

Not Met

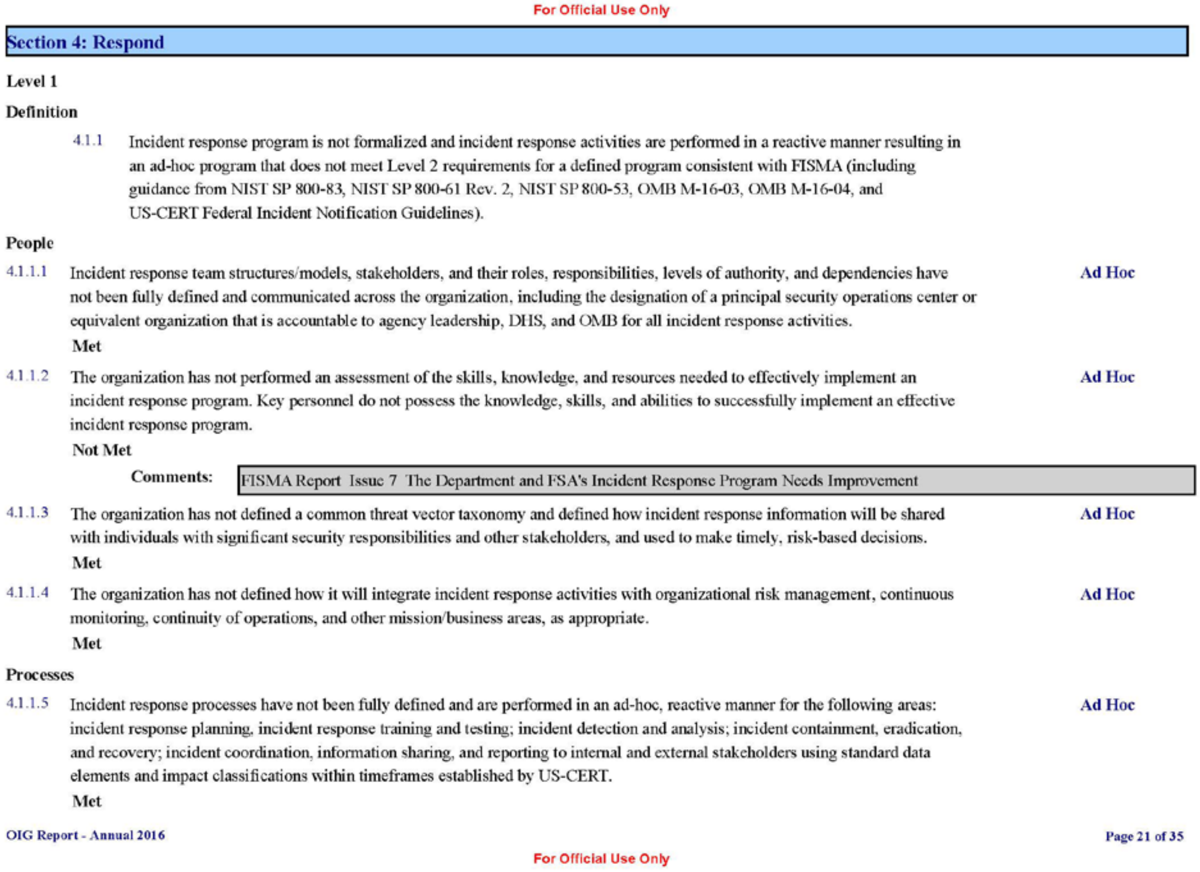
Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

3.5.1.7 The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its ISCM program. **Optimized**

Not Met

Comments: FISMA Report Issue 6 The Department's and FSA's ISCM Program Needs Improvement (Repeat Finding)

Level	Score	Possible Score
LEVEL 1: Ad-hoc	3	20



For Official Use Only

Section 4: Respond

Level 1

Definition

4.1.1 Incident response program is not formalized and incident response activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines).

People

4.1.1.1 Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have not been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities. **Ad Hoc**

Met

4.1.1.2 The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. Key personnel do not possess the knowledge, skills, and abilities to successfully implement an effective incident response program. **Ad Hoc**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.1.1.3 The organization has not defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders, and used to make timely, risk-based decisions. **Ad Hoc**

Met

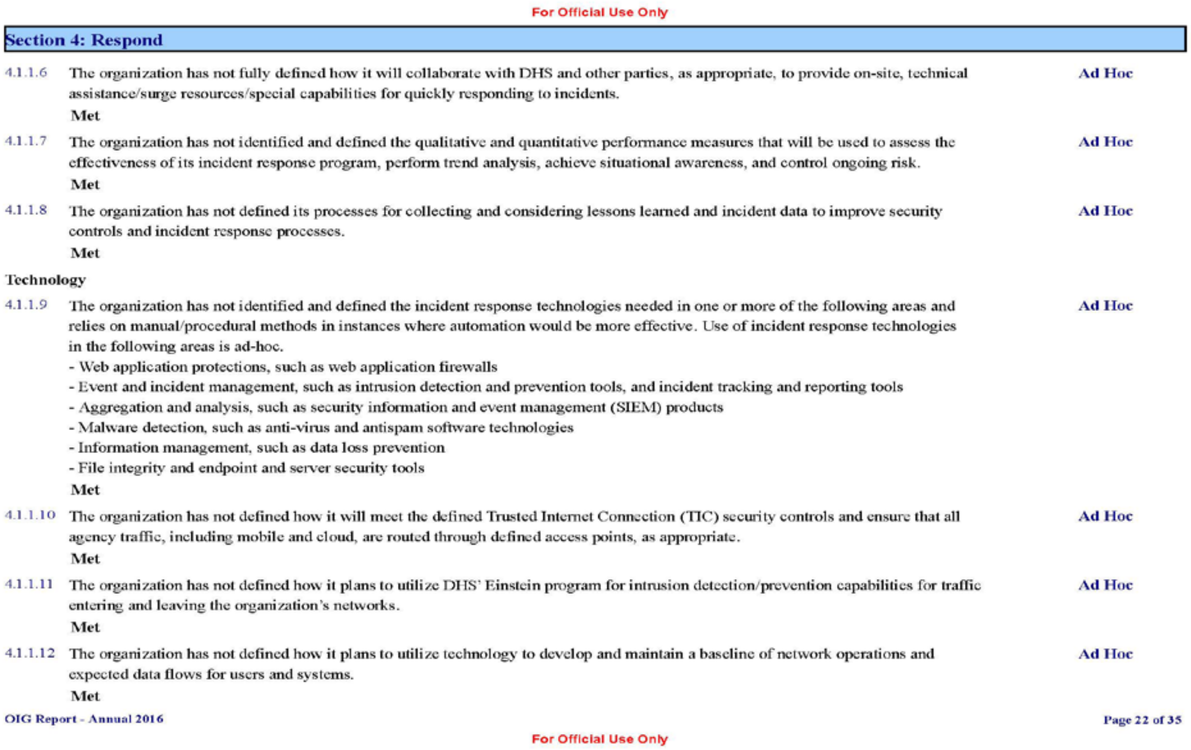
4.1.1.4 The organization has not defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. **Ad Hoc**

Met

Processes

4.1.1.5 Incident response processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting to internal and external stakeholders using standard data elements and impact classifications within timeframes established by US-CERT. **Ad Hoc**

Met



Section 4: Respond

4.1.1.6 The organization has not fully defined how it will collaborate with DHS and other parties, as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents.
Ad Hoc

Met

4.1.1.7 The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk.
Ad Hoc

Met

4.1.1.8 The organization has not defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes.
Ad Hoc

Met

Technology

4.1.1.9 The organization has not identified and defined the incident response technologies needed in one or more of the following areas and relies on manual/procedural methods in instances where automation would be more effective. Use of incident response technologies in the following areas is ad-hoc.
Ad Hoc

- 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 anti-virus and antispam software technologies
- Information management, such as data loss prevention
- File integrity and endpoint and server security tools

Met

4.1.1.10 The organization has not defined how it will meet the defined Trusted Internet Connection (TIC) security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate.
Ad Hoc

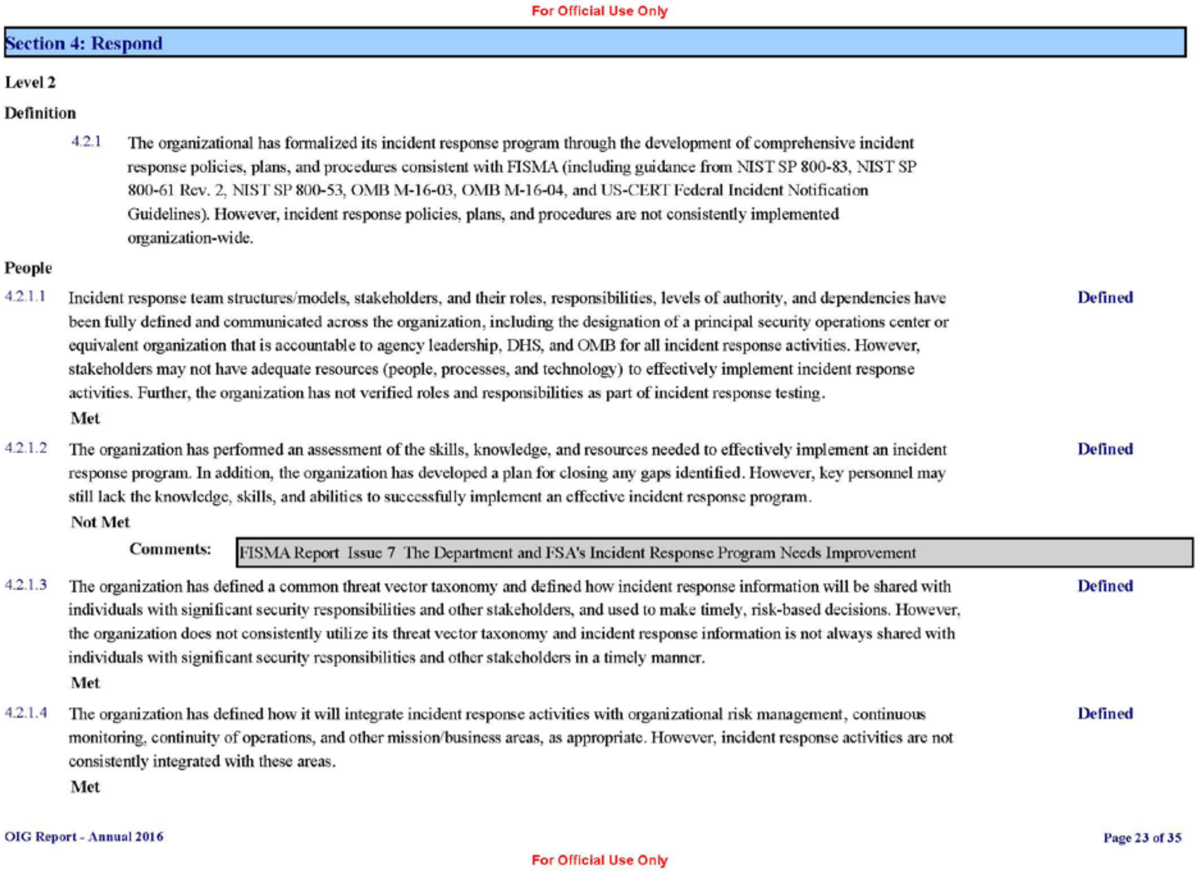
Met

4.1.1.11 The organization has not defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving the organization's networks.
Ad Hoc

Met

4.1.1.12 The organization has not defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems.
Ad Hoc

Met



Section 4: Respond

Level 2

Definition

4.2.1 The organizational has formalized its incident response program through the development of comprehensive incident response policies, plans, and procedures consistent with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines). However, incident response policies, plans, and procedures are not consistently implemented organization-wide.

People

4.2.1.1 Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities. However, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement incident response activities. Further, the organization has not verified roles and responsibilities as part of incident response testing.
Defined

Met

4.2.1.2 The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. In addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective incident response program.
Defined

Not Met

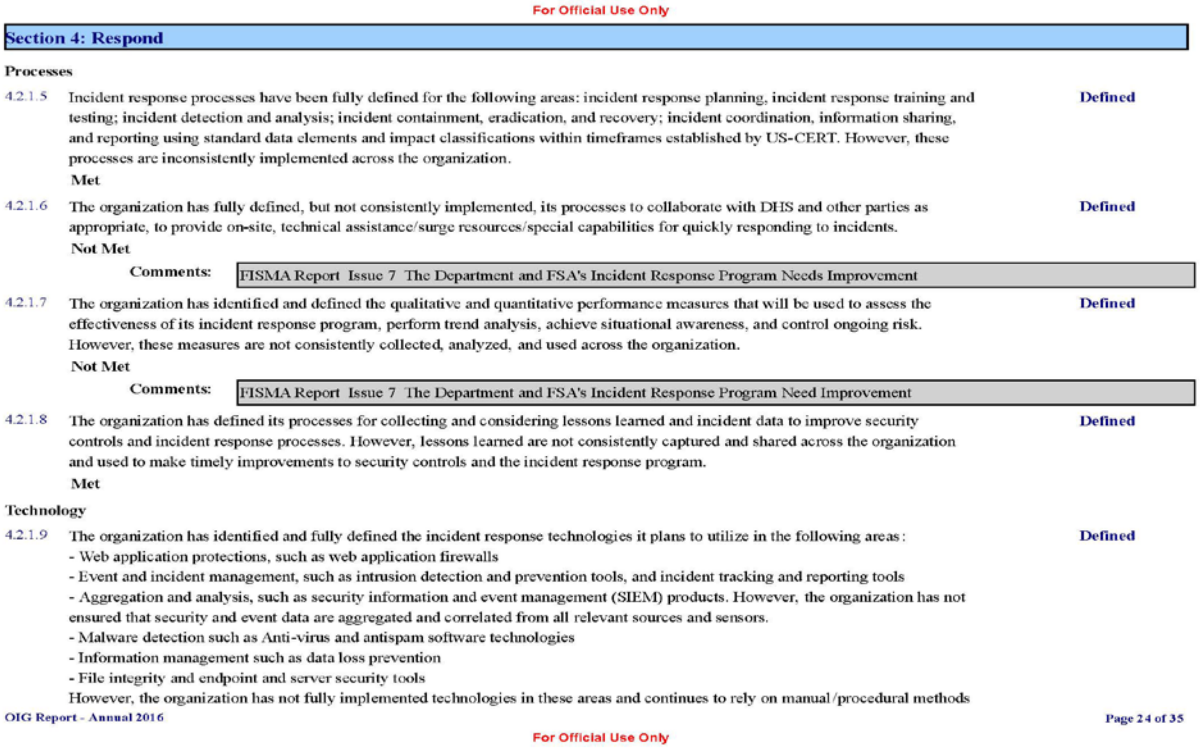
Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.2.1.3 The organization has defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders, and used to make timely, risk-based decisions. However, the organization does not consistently utilize its threat vector taxonomy and incident response information is not always shared with individuals with significant security responsibilities and other stakeholders in a timely manner.
Defined

Met

4.2.1.4 The organization has defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. However, incident response activities are not consistently integrated with these areas.
Defined

Met



Section 4: Respond

Processes

4.2.1.5 Incident response processes have been fully defined for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting using standard data elements and impact classifications within timeframes established by US-CERT. However, these processes are inconsistently implemented across the organization. **Defined**

Met

4.2.1.6 The organization has fully defined, but not consistently implemented, its processes to collaborate with DHS and other parties as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents. **Defined**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.2.1.7 The organization has identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. **Defined**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Need Improvement

4.2.1.8 The organization has defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes. However, lessons learned are not consistently captured and shared across the organization and used to make timely improvements to security controls and the incident response program. **Defined**

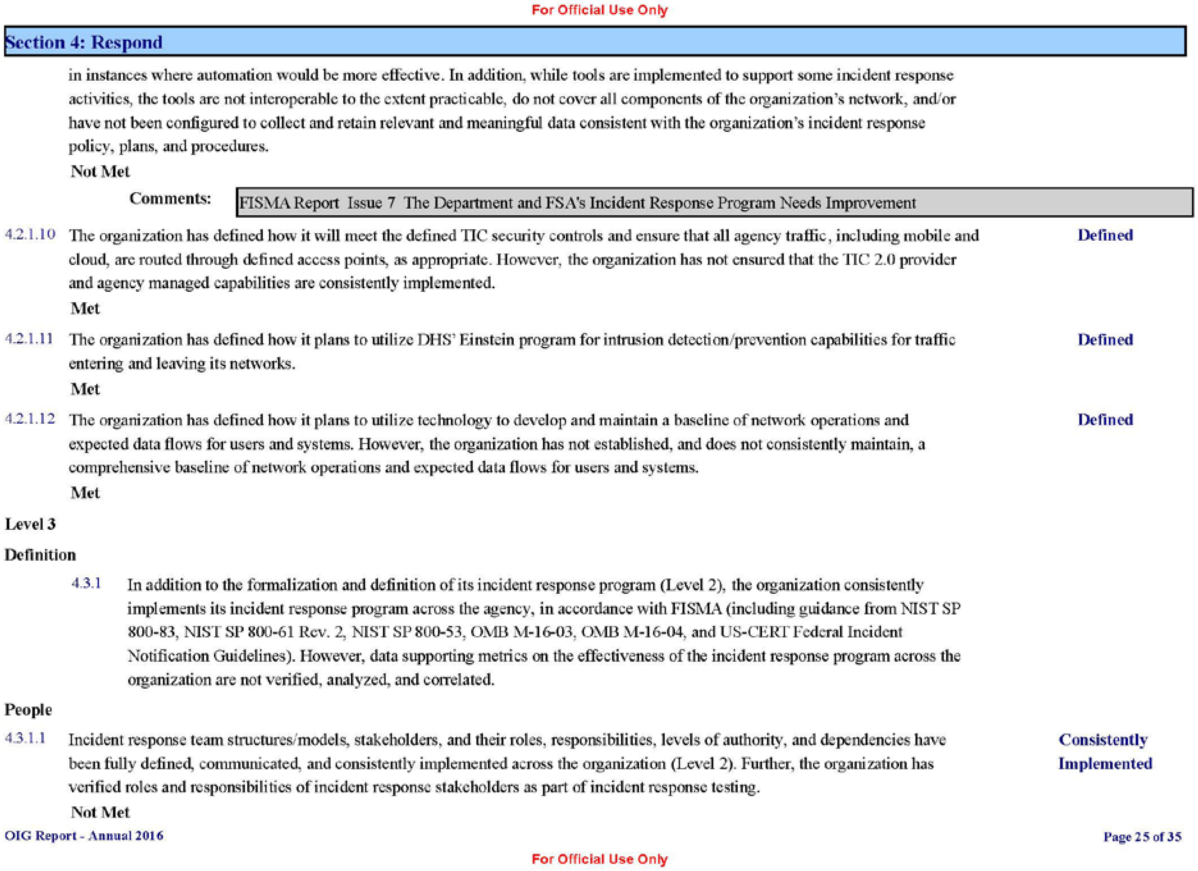
Met

Technology

4.2.1.9 The organization has identified and fully defined the incident response technologies it plans to utilize in the following areas: **Defined**

- 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. However, the organization has not ensured that security and event data are aggregated and correlated from all relevant sources and sensors.
- Malware detection such as Anti-virus and antispam software technologies
- Information management such as data loss prevention
- File integrity and endpoint and server security tools

However, the organization has not fully implemented technologies in these areas and continues to rely on manual/procedural methods



Section 4: Respond

in instances where automation would be more effective. In addition, while tools are implemented to support some incident response activities, the tools are not interoperable to the extent practicable, do not cover all components of the organization's network, and/or have not been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, plans, and procedures.

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.2.1.10 The organization has defined how it will meet the defined TIC security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. However, the organization has not ensured that the TIC 2.0 provider and agency managed capabilities are consistently implemented. **Defined**

Met

4.2.1.11 The organization has defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving its networks. **Defined**

Met

4.2.1.12 The organization has defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems. However, the organization has not established, and does not consistently maintain, a comprehensive baseline of network operations and expected data flows for users and systems. **Defined**

Met

Level 3

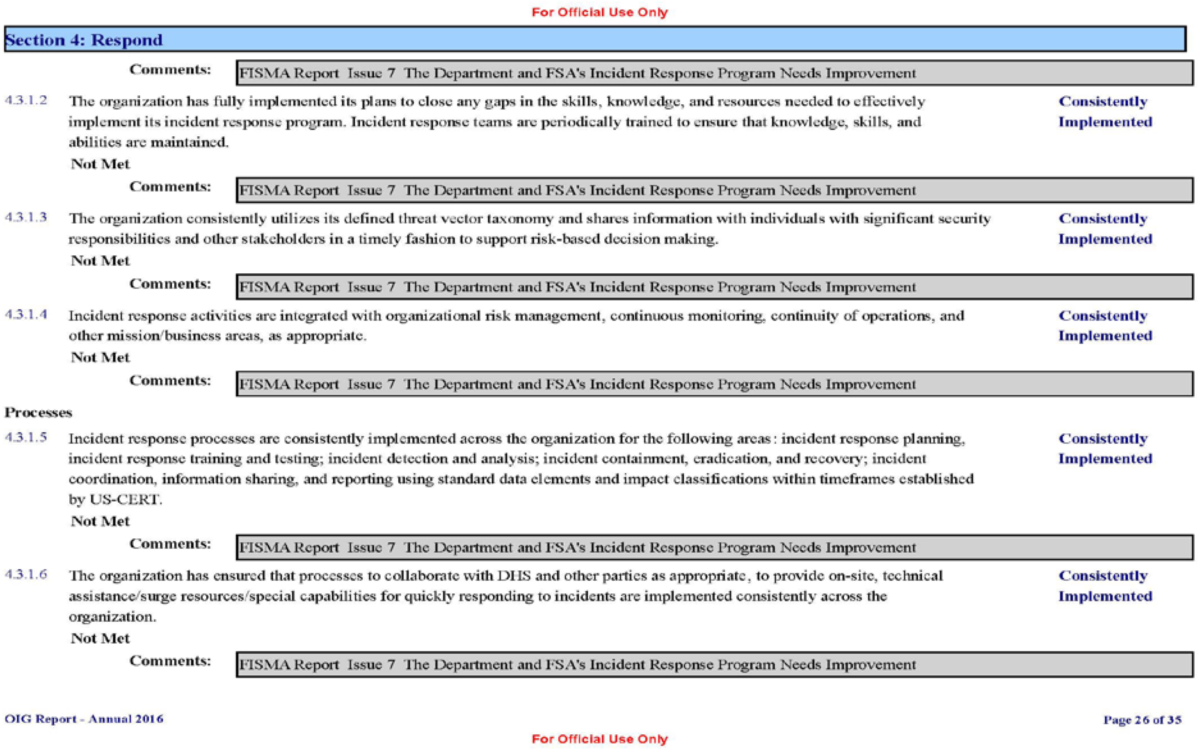
Definition

4.3.1 In addition to the formalization and definition of its incident response program (Level 2), the organization consistently implements its incident response program across the agency, in accordance with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines). However, data supporting metrics on the effectiveness of the incident response program across the organization are not verified, analyzed, and correlated.

People

4.3.1.1 Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined, communicated, and consistently implemented across the organization (Level 2). Further, the organization has verified roles and responsibilities of incident response stakeholders as part of incident response testing. **Consistently Implemented**

Not Met



Section 4: Respond

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.3.1.2 The organization has fully implemented its plans to close any gaps in the skills, knowledge, and resources needed to effectively implement its incident response program. Incident response teams are periodically trained to ensure that knowledge, skills, and abilities are maintained. **Consistently Implemented**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.3.1.3 The organization consistently utilizes its defined threat vector taxonomy and shares information with individuals with significant security responsibilities and other stakeholders in a timely fashion to support risk-based decision making. **Consistently Implemented**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.3.1.4 Incident response activities are integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. **Consistently Implemented**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

Processes

4.3.1.5 Incident response processes are consistently implemented across the organization for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting using standard data elements and impact classifications within timeframes established by US-CERT. **Consistently Implemented**

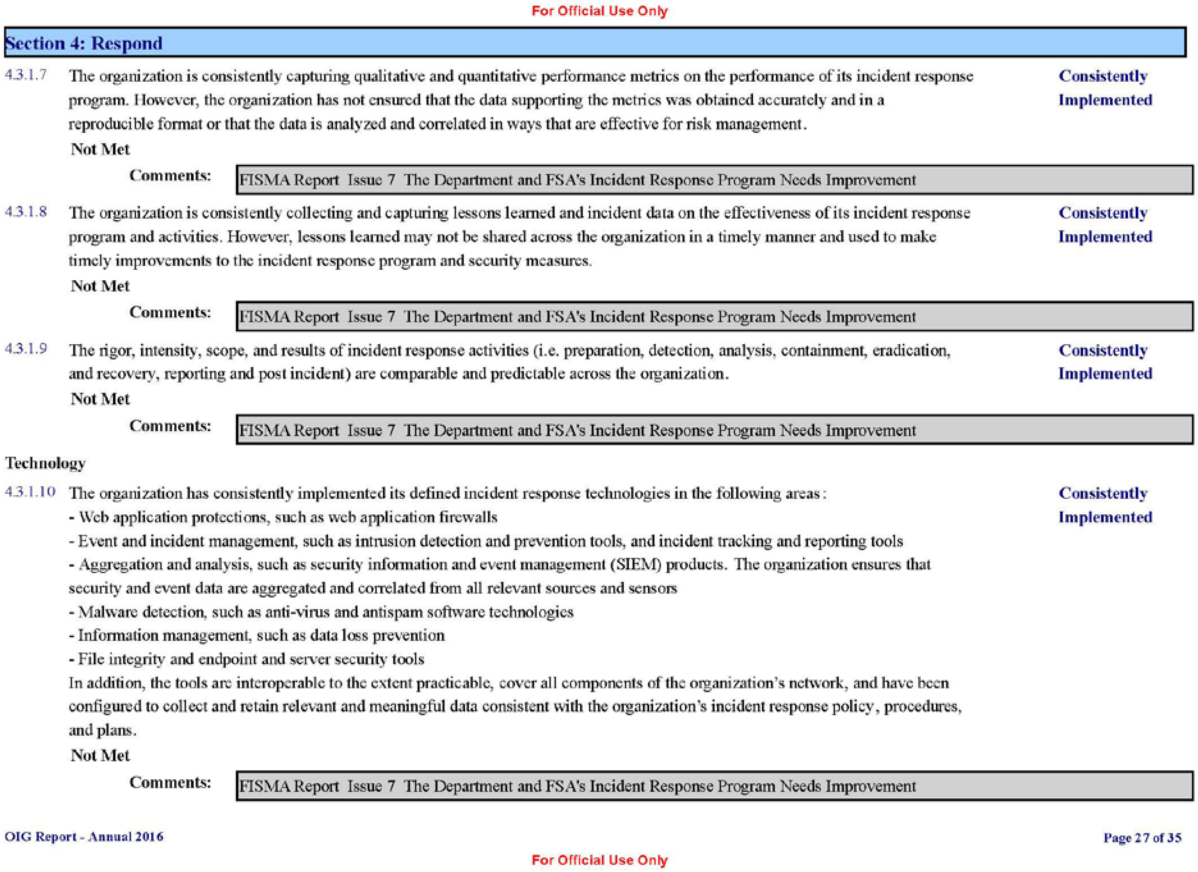
Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.3.1.6 The organization has ensured that processes to collaborate with DHS and other parties as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents are implemented consistently across the organization. **Consistently Implemented**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement



Section 4: Respond

4.3.1.7 The organization is consistently capturing qualitative and quantitative performance metrics on the performance of its incident response program. However, the organization has not ensured that the data supporting the metrics was obtained accurately and in a reproducible format or that the data is analyzed and correlated in ways that are effective for risk management. **Consistently Implemented**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.3.1.8 The organization is consistently collecting and capturing lessons learned and incident data on the effectiveness of its incident response program and activities. However, lessons learned may not be shared across the organization in a timely manner and used to make timely improvements to the incident response program and security measures. **Consistently Implemented**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.3.1.9 The rigor, intensity, scope, and results of incident response activities (i.e. preparation, detection, analysis, containment, eradication, and recovery, reporting and post incident) are comparable and predictable across the organization. **Consistently Implemented**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

Technology

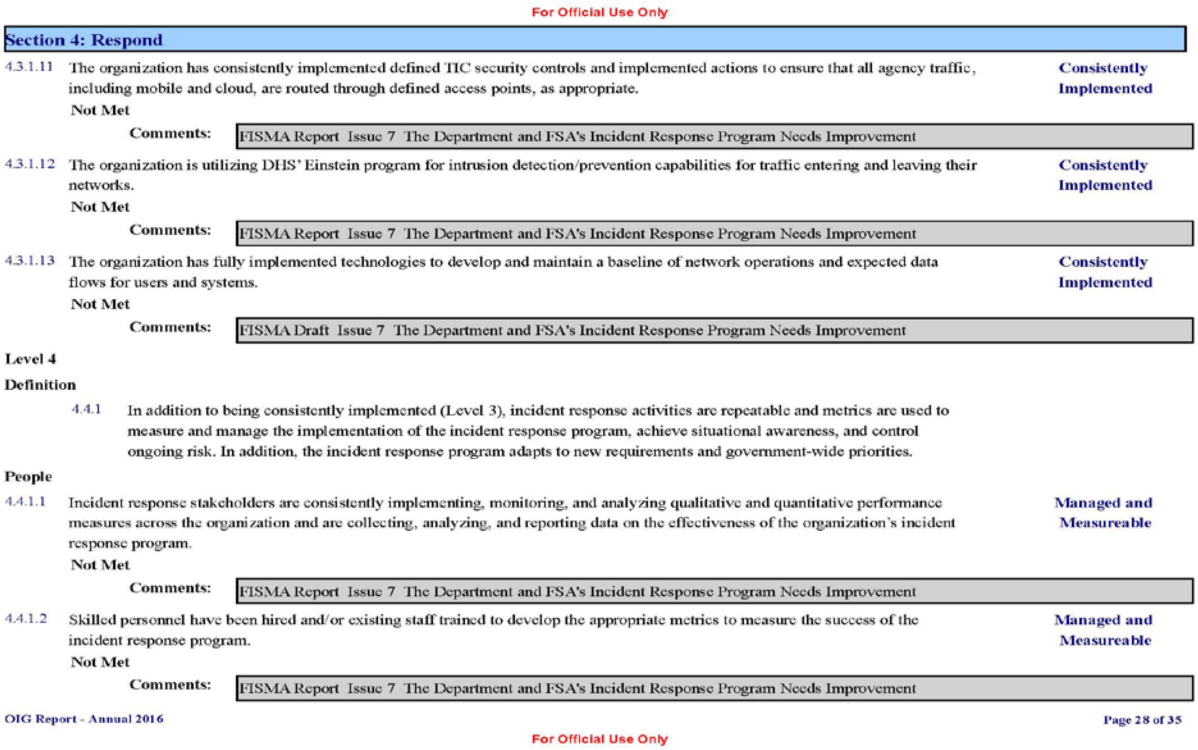
4.3.1.10 The organization has consistently implemented its defined incident response technologies in the following areas: **Consistently Implemented**

- 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. The organization ensures that security and event data are aggregated and correlated from all relevant sources and sensors
- Malware detection, such as anti-virus and antispam software technologies
- Information management, such as data loss prevention
- File integrity and endpoint and server security tools

In addition, the tools are interoperable to the extent practicable, cover all components of the organization's network, and have been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, procedures, and plans.

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement



For Official Use Only

Section 4: Respond

4.3.1.11 The organization has consistently implemented defined TIC security controls and implemented actions to ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. **Consistently Implemented**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.3.1.12 The organization is utilizing DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving their networks. **Consistently Implemented**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.3.1.13 The organization has fully implemented technologies to develop and maintain a baseline of network operations and expected data flows for users and systems. **Consistently Implemented**

Not Met

Comments: FISMA Draft Issue 7 The Department and FSA's Incident Response Program Needs Improvement

Level 4

Definition

4.4.1 In addition to being consistently implemented (Level 3), incident response activities are repeatable and metrics are used to measure and manage the implementation of the incident response program, achieve situational awareness, and control ongoing risk. In addition, the incident response program adapts to new requirements and government-wide priorities.

People

4.4.1.1 Incident response stakeholders are consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and are collecting, analyzing, and reporting data on the effectiveness of the organization's incident response program. **Managed and Measureable**

Not Met

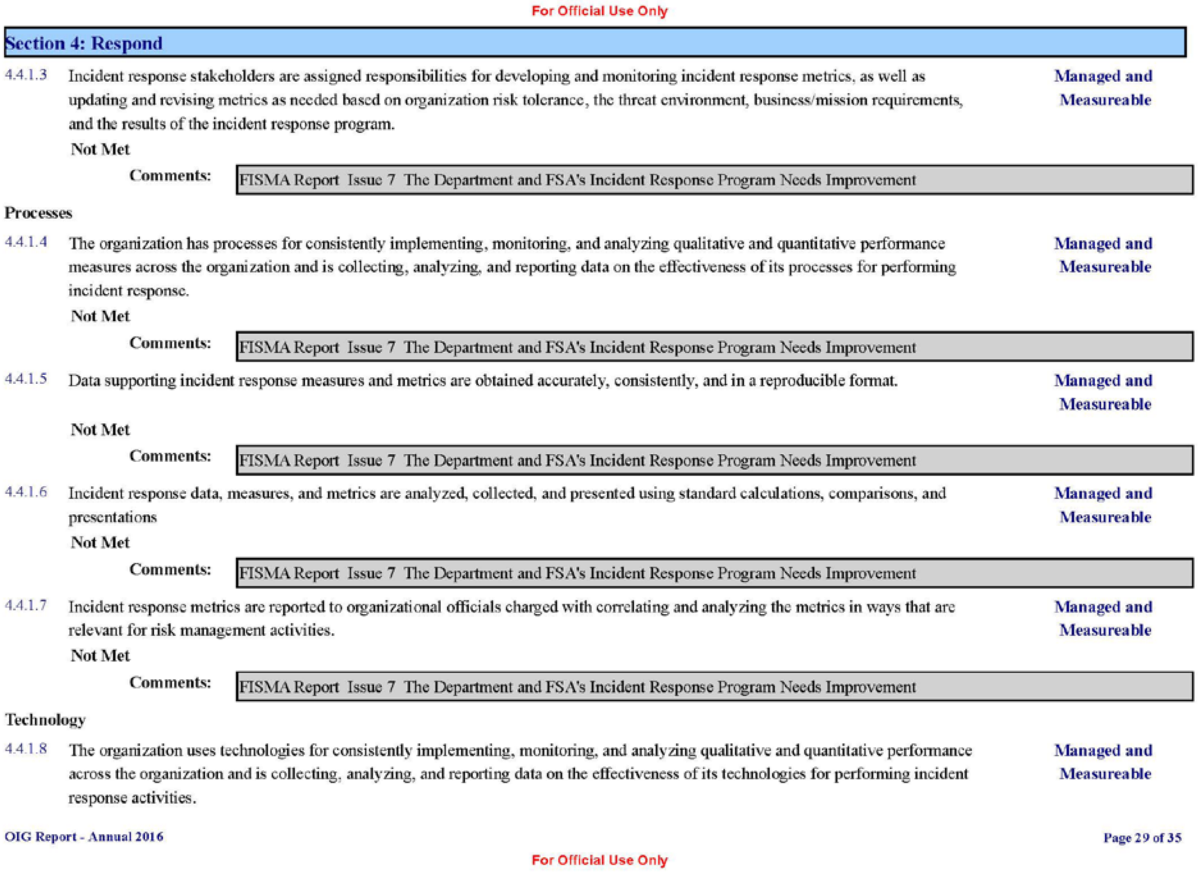
Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.4.1.2 Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the incident response program. **Managed and Measureable**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

For Official Use Only



For Official Use Only

Section 4: Respond

4.4.1.3 Incident response stakeholders are assigned responsibilities for developing and monitoring incident response metrics, as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the incident response program. **Managed and Measureable**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

Processes

4.4.1.4 The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing incident response. **Managed and Measureable**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.4.1.5 Data supporting incident response measures and metrics are obtained accurately, consistently, and in a reproducible format. **Managed and Measureable**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.4.1.6 Incident response data, measures, and metrics are analyzed, collected, and presented using standard calculations, comparisons, and presentations **Managed and Measureable**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.4.1.7 Incident response metrics are reported to organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities. **Managed and Measureable**

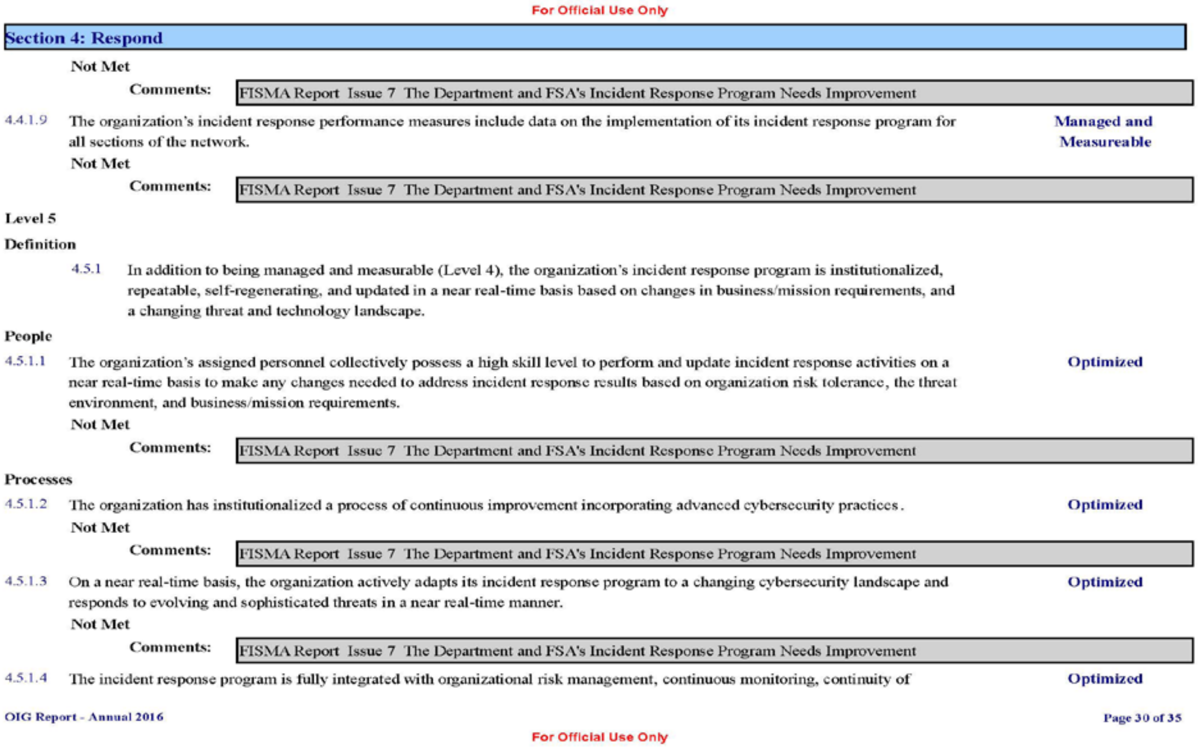
Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

Technology

4.4.1.8 The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing incident response activities. **Managed and Measureable**

For Official Use Only



Section 4: Respond

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.4.1.9 The organization's incident response performance measures include data on the implementation of its incident response program for all sections of the network. **Managed and Measureable**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

Level 5

Definition

4.5.1 In addition to being managed and measurable (Level 4), the organization's incident response program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements, and a changing threat and technology landscape.

People

4.5.1.1 The organization's assigned personnel collectively possess a high skill level to perform and update incident response activities on a near real-time basis to make any changes needed to address incident response results based on organization risk tolerance, the threat environment, and business/mission requirements. **Optimized**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

Processes

4.5.1.2 The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity practices. **Optimized**

Not Met

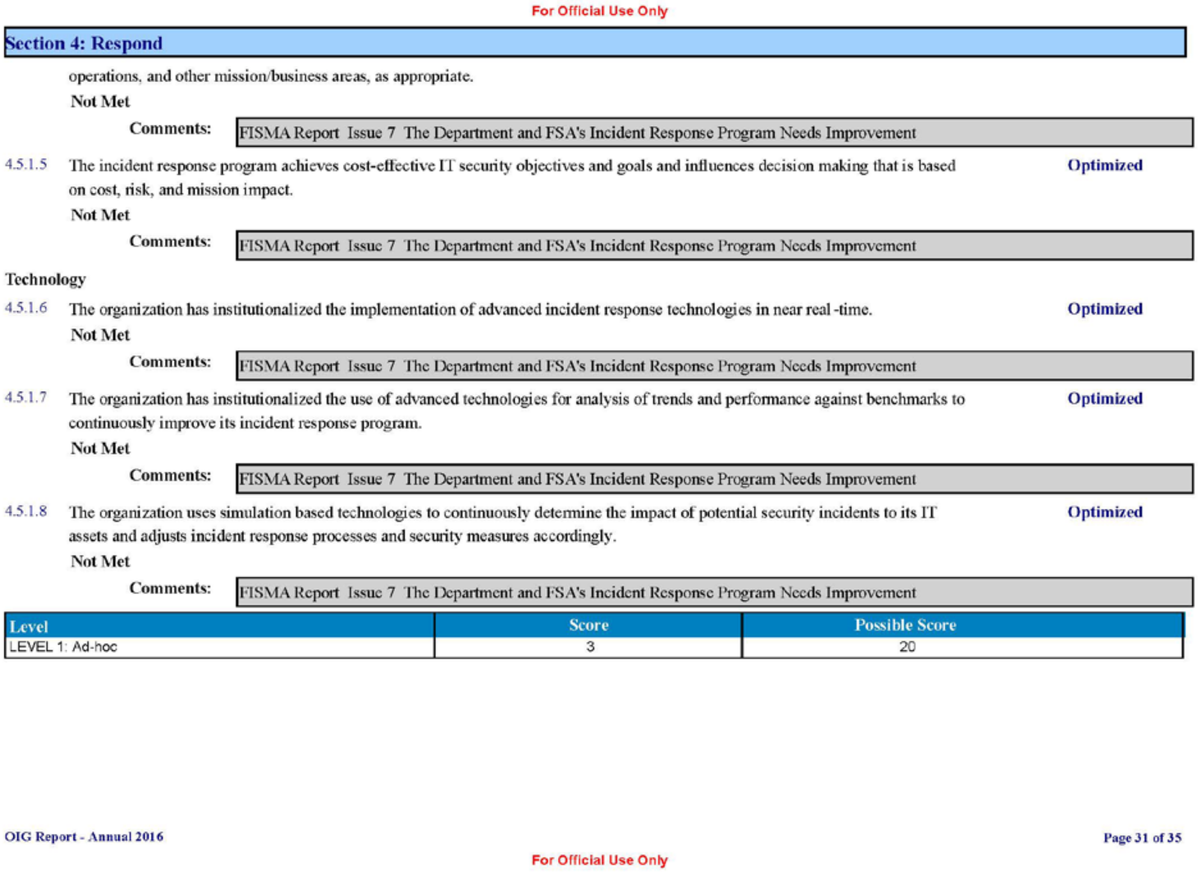
Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.5.1.3 On a near real-time basis, the organization actively adapts its incident response program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a near real-time manner. **Optimized**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.5.1.4 The incident response program is fully integrated with organizational risk management, continuous monitoring, continuity of **Optimized**



Section 4: Respond

operations, and other mission/business areas, as appropriate.

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.5.1.5 The incident response program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact. **Optimized**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

Technology

4.5.1.6 The organization has institutionalized the implementation of advanced incident response technologies in near real -time. **Optimized**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.5.1.7 The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its incident response program. **Optimized**

Not Met

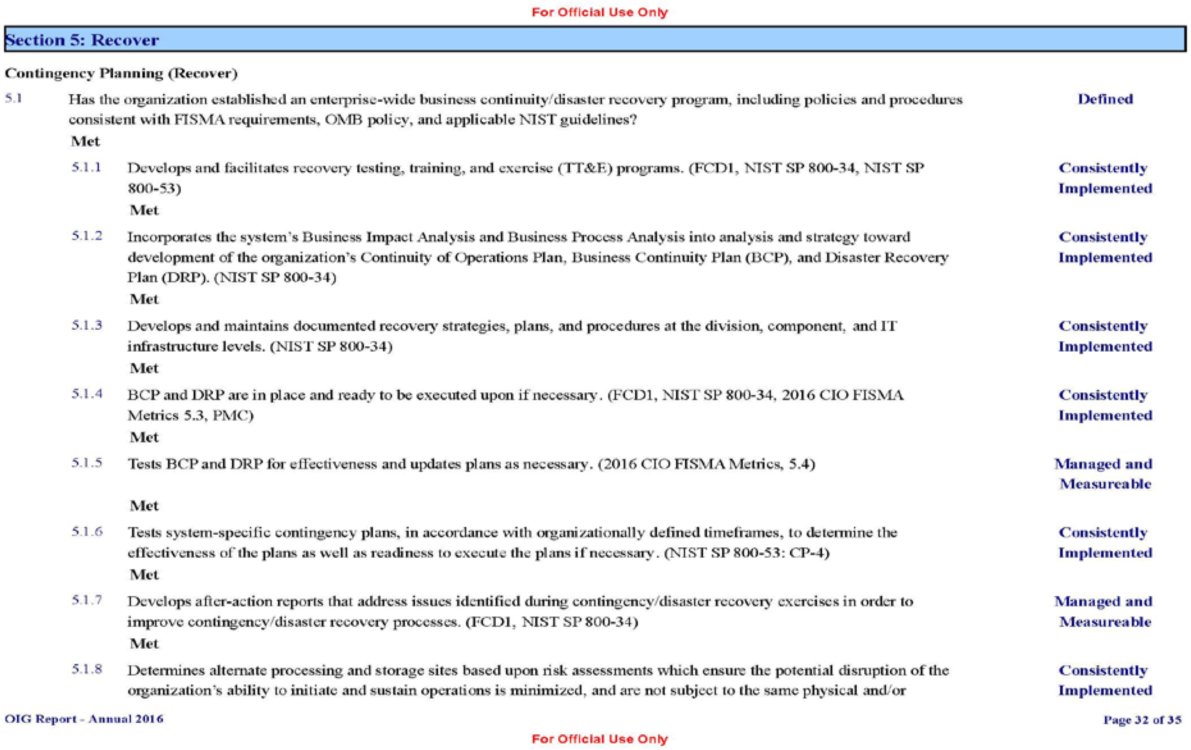
Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

4.5.1.8 The organization uses simulation based technologies to continuously determine the impact of potential security incidents to its IT assets and adjusts incident response processes and security measures accordingly. **Optimized**

Not Met

Comments: FISMA Report Issue 7 The Department and FSA's Incident Response Program Needs Improvement

Level	Score	Possible Score
LEVEL 1: Ad-hoc	3	20



Section 5: Recover

Contingency Planning (Recover)

5.1 Has the organization established an enterprise-wide business continuity/disaster recovery program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? — **Defined**

Met

5.1.1 Develops and facilitates recovery testing, training, and exercise (TT&E) programs. (FCD1, NIST SP 800-34, NIST SP 800-53) — **Consistently Implemented**

Met

5.1.2 Incorporates the system's Business Impact Analysis and Business Process Analysis into analysis and strategy toward development of the organization's Continuity of Operations Plan, Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP). (NIST SP 800-34) — **Consistently Implemented**

Met

5.1.3 Develops and maintains documented recovery strategies, plans, and procedures at the division, component, and IT infrastructure levels. (NIST SP 800-34) — **Consistently Implemented**

Met

5.1.4 BCP and DRP are in place and ready to be executed upon if necessary. (FCD1, NIST SP 800-34, 2016 CIO FISMA Metrics 5.3, PMC) — **Consistently Implemented**

Met

5.1.5 Tests BCP and DRP for effectiveness and updates plans as necessary. (2016 CIO FISMA Metrics, 5.4) — **Managed and Measureable**

Met

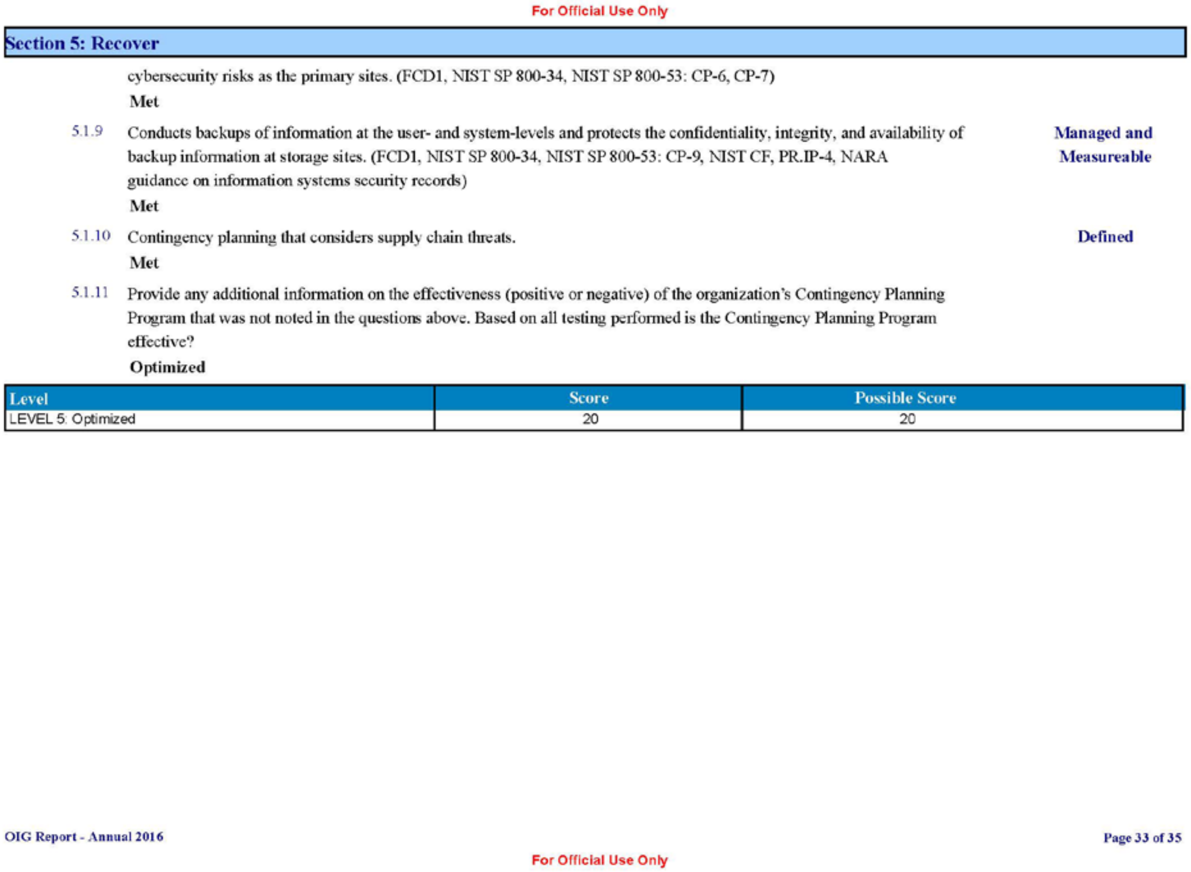
5.1.6 Tests system-specific contingency plans, in accordance with organizationally defined timeframes, to determine the effectiveness of the plans as well as readiness to execute the plans if necessary. (NIST SP 800-53: CP-4) — **Consistently Implemented**

Met

5.1.7 Develops after-action reports that address issues identified during contingency/disaster recovery exercises in order to improve contingency/disaster recovery processes. (FCD1, NIST SP 800-34) — **Managed and Measureable**

Met

5.1.8 Determines alternate processing and storage sites based upon risk assessments which ensure the potential disruption of the organization's ability to initiate and sustain operations is minimized, and are not subject to the same physical and/or — **Consistently Implemented**



Section 5: Recover

cybersecurity risks as the primary sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-6, CP-7)

Met

5.1.9 Conducts backups of information at the user- and system-levels and protects the confidentiality, integrity, and availability of backup information at storage sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-9, NIST CF, PR.IP-4, NARA guidance on information systems security records) — **Managed and Measureable**

Met

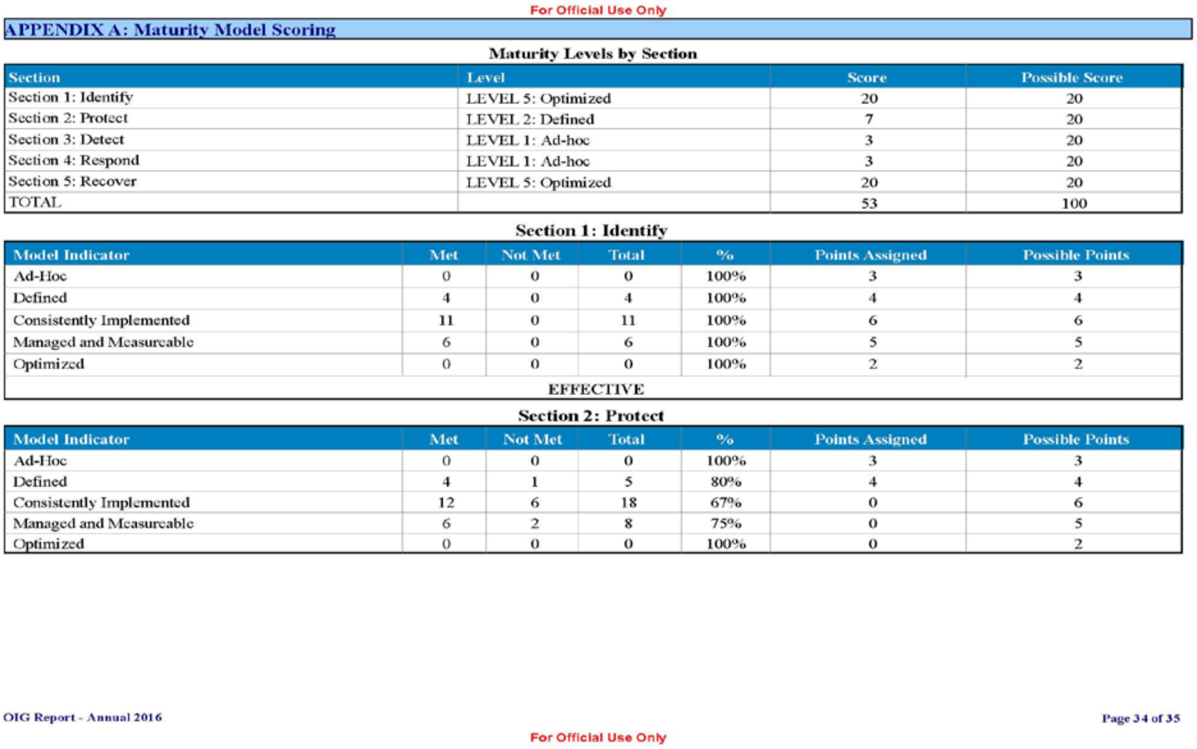
5.1.10 Contingency planning that considers supply chain threats. — **Defined**

Met

5.1.11 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. Based on all testing performed is the Contingency Planning Program effective?

Optimized

Level	Score	Possible Score
LEVEL 5: Optimized	20	20



For Official Use Only

APPENDIX A: Maturity Model Scoring

Maturity Levels by Section

Section	Level	Score	Possible Score
Section 1: Identify	LEVEL 5: Optimized	20	20
Section 2: Protect	LEVEL 2: Defined	7	20
Section 3: Detect	LEVEL 1: Ad-hoc	3	20
Section 4: Respond	LEVEL 1: Ad-hoc	3	20
Section 5: Recover	LEVEL 5: Optimized	20	20
TOTAL		53	100

Section 1: Identify

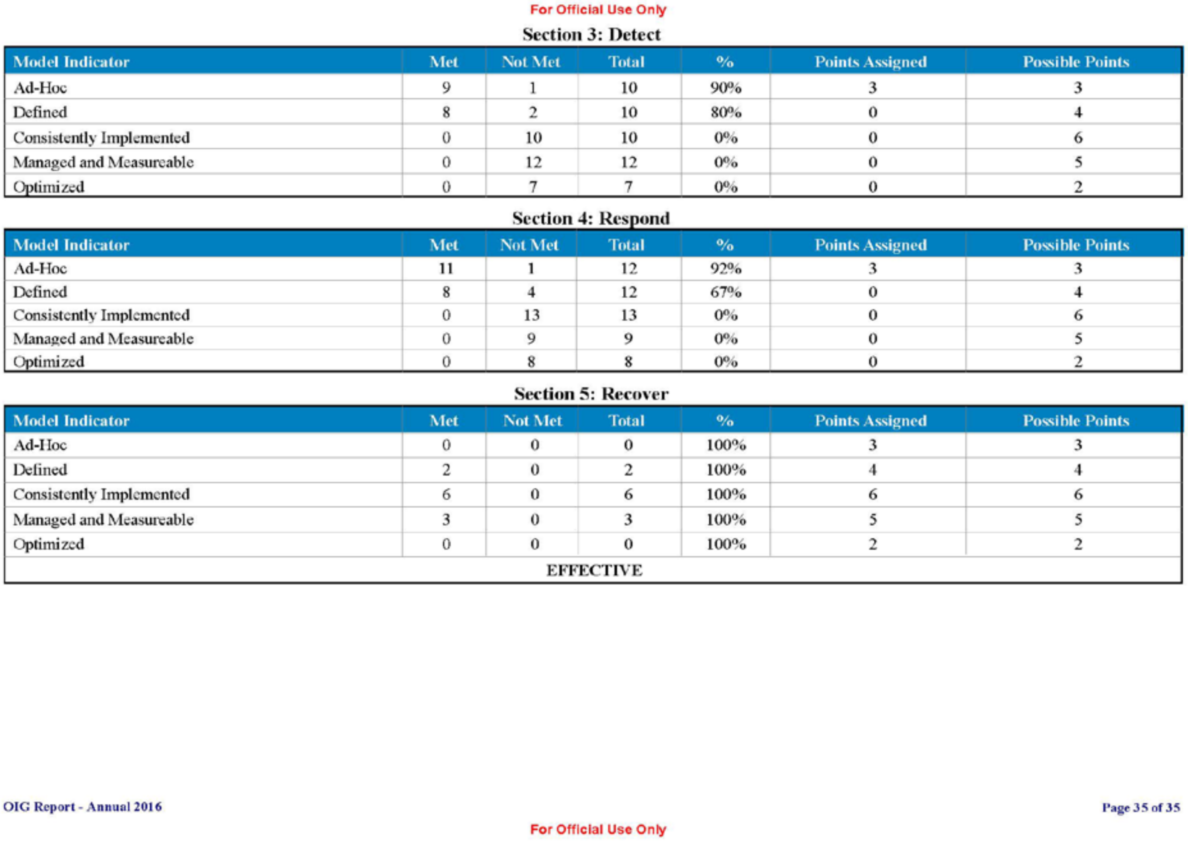
Model Indicator	Met	Not Met	Total	%	Points Assigned	Possible Points
Ad-Hoc	0	0	0	100%	3	3
Defined	4	0	4	100%	4	4
Consistently Implemented	11	0	11	100%	6	6
Managed and Measureable	6	0	6	100%	5	5
Optimized	0	0	0	100%	2	2
EFFECTIVE						

Section 2: Protect

Model Indicator	Met	Not Met	Total	%	Points Assigned	Possible Points
Ad-Hoc	0	0	0	100%	3	3
Defined	4	1	5	80%	4	4
Consistently Implemented	12	6	18	67%	0	6
Managed and Measureable	6	2	8	75%	0	5
Optimized	0	0	0	100%	0	2

OIG Report - Annual 2016 Page 34 of 35

For Official Use Only



For Official Use Only

Section 3: Detect

Model Indicator	Met	Not Met	Total	%	Points Assigned	Possible Points
Ad-Hoc	9	1	10	90%	3	3
Defined	8	2	10	80%	0	4
Consistently Implemented	0	10	10	0%	0	6
Managed and Measureable	0	12	12	0%	0	5
Optimized	0	7	7	0%	0	2

Section 4: Respond

Model Indicator	Met	Not Met	Total	%	Points Assigned	Possible Points
Ad-Hoc	11	1	12	92%	3	3
Defined	8	4	12	67%	0	4
Consistently Implemented	0	13	13	0%	0	6
Managed and Measureable	0	9	9	0%	0	5
Optimized	0	8	8	0%	0	2

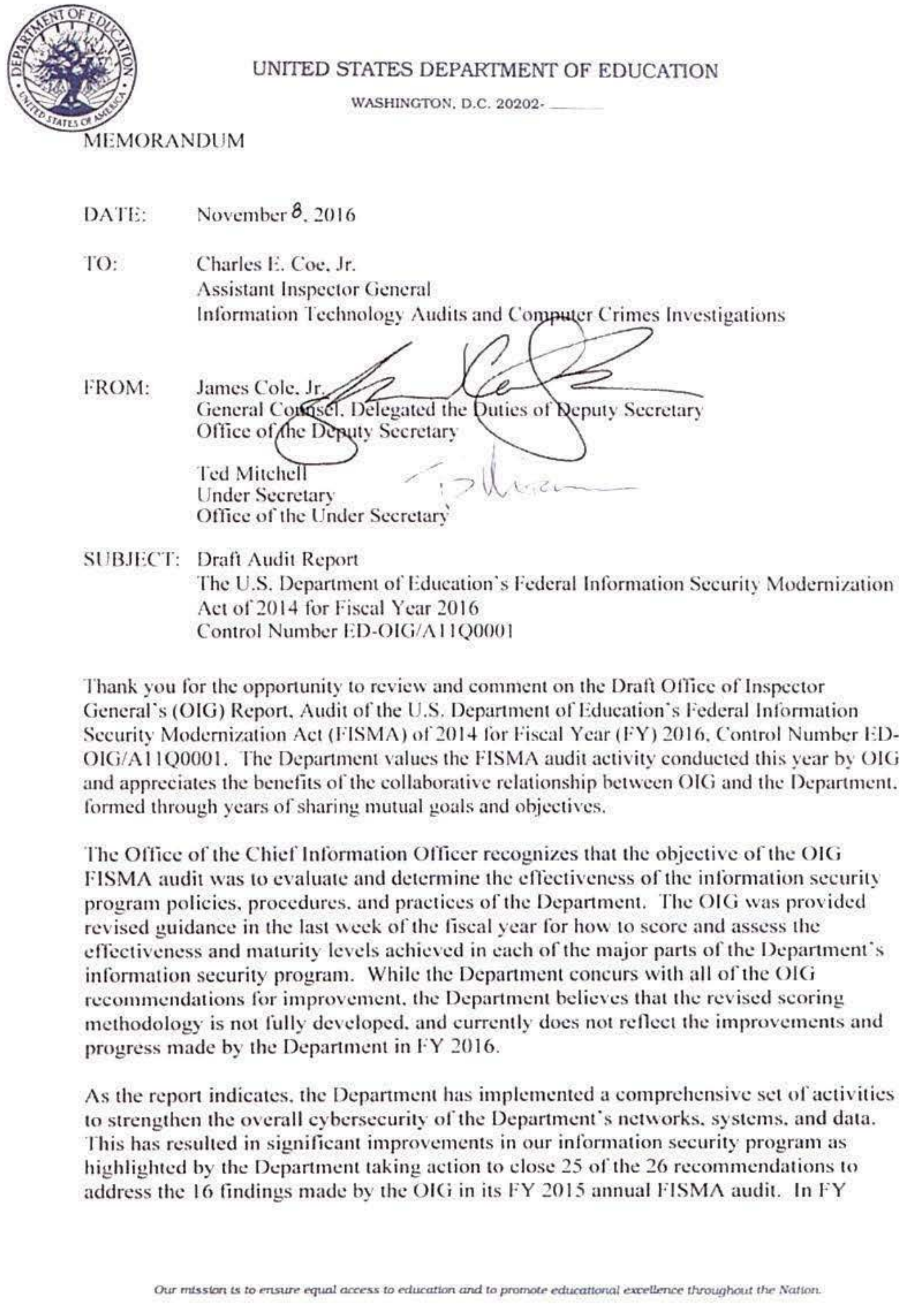
Section 5: Recover

Model Indicator	Met	Not Met	Total	%	Points Assigned	Possible Points
Ad-Hoc	0	0	0	100%	3	3
Defined	2	0	2	100%	4	4
Consistently Implemented	6	0	6	100%	6	6
Managed and Measureable	3	0	3	100%	5	5
Optimized	0	0	0	100%	2	2
EFFECTIVE						

OIG Report - Annual 2016 Page 35 of 35

For Official Use Only

Enclosure 2: Management Comments



UNITED STATES DEPARTMENT OF EDUCATION

WASHINGTON, D.C. 20202-

MEMORANDUM

DATE: November 8, 2016

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

FROM: James Cole, Jr.
General Counsel, Delegated the Duties of Deputy Secretary
Office of the Deputy Secretary

Ted Mitchell
Under Secretary
Office of the Under Secretary

SUBJECT: Draft Audit Report
The U.S. Department of Education's Federal Information Security Modernization Act of 2014 for Fiscal Year 2016
Control Number ED-OIG/A11Q0001

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) 2016, Control Number ED-OIG/A11Q0001. The Department values the FISMA audit activity conducted this year by OIG and appreciates the benefits of the collaborative relationship between OIG and the Department, formed through years of sharing mutual goals and objectives.

The Office of the Chief Information Officer recognizes that the objective of the OIG FISMA audit was to evaluate and determine the effectiveness of the information security program policies, procedures, and practices of the Department. The OIG was provided revised guidance in the last week of the fiscal year for how to score and assess the effectiveness and maturity levels achieved in each of the major parts of the Department's information security program. While the Department concurs with all of the OIG recommendations for improvement, the Department believes that the revised scoring methodology is not fully developed, and currently does not reflect the improvements and progress made by the Department in FY 2016.

As the report indicates, the Department has implemented a comprehensive set of activities to strengthen the overall cybersecurity of the Department's networks, systems, and data. This has resulted in significant improvements in our information security program as highlighted by the Department taking action to close 25 of the 26 recommendations to address the 16 findings made by the OIG in its FY 2015 annual FISMA audit. In FY

2016, the OIG is only reporting 15 recommendations to address 11 findings, which reflects a noteworthy drop in the total number of findings and recommendations from the previous reporting year.

As with recommendations made in prior year audits, the Department has garnered significant benefits. The Department expects that the recommendations presented in this audit will further improve the effectiveness of the information security program. Each finding and recommendation will be addressed in the plan provided, and as agreed upon by your office.

The following responses address each recommendation:

REPORTING METRIC DOMAIN No. 3: Configuration Management

OIG Recommendation: 3.1. Ensure that policies and procedures are reviewed and revised at least annually, or as needed. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation and has taken great strides during FY 2016 to improve Configuration Management. The Department has renewed efforts to ensure guidance is updated. For example, the OCIO updated OCIO-01, "Handbook for Information Assurance Security Policy, OCIO Information Technology Security Risk Assessment Procedures," and "Cybersecurity Risk Assessment and Authorization Guide". In addition, with continuing reviews of current policy, the Office of the Chief Information Officer (OCIO) will define a process for the vetting of Department Cybersecurity Guidance. This process will be defined and implemented by the end of FY 2017. (Planned Completion: September 2017)

OIG Recommendation: 3.2. Update the outdated configuration management policies and procedures to reflect current NIST and industry standards. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. OCIO will revise Department Configuration Management policies and procedures to reflect current NIST and industry standards. This activity will be completed by the end of FY 2017. (Planned Completion: September 2017)

OIG Recommendation: 3.3. Immediately establish TLS 1.1 or higher as the only connection for all Department connections. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation and has taken great strides during FY 2016 to improve Configuration Management. The Department has worked with System Owners throughout FY 2016 to resolve this vulnerability and the Department expects to resolve this finding by December 30, 2016. In addition, the Department will issue guidance that is aligned with NIST Special Publication 800-52 Rev 1, (Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations). The policy guidance will establish that the implementation of properly configured TLS versions 1.1 and 1.2 for the protection of Department and Federal information is required. The policy guidance will be developed and issued prior to January 31, 2017. (Planned Completion: January 2017). For information, the Department will concurrently develop migration plans to TLS1.2, configured using approved schemes and algorithms, by June 1, 2017.

OIG Recommendation: 3.4. Enable the network access control solution to validate and restrict personal devices from connecting to the Department's internal network. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation and has taken great strides during FY 2016 to improve Configuration Management. The Department began the deployment of a network access control (NAC) solution in FY 2015 and is working with contract teams to validate the current configuration and adjust if required to properly restrict access to internal networks for the EDUCATE and VDC environments. The Department will continue the effort to enable network access control to validate and restrict personal devices from connecting to the Department's internal network. This activity will be completed by February 28, 2017. (Planned Completion: February 2017)

OIG Recommendation: 3.5. Immediately correct or mitigate the vulnerabilities identified during the vulnerability assessment.

Management Response: The Department concurs with this recommendation. The Department will develop a plan to address the identified findings within 30 days of receiving the final report. OCIO will work with system owners to create POA&M(s) for any finding that cannot be addressed within an acceptable timeframe. This activity will be completed within 30 days of receiving the final report. The completion date for the correction and mitigation of the vulnerabilities identified by OIG during the OIG vulnerability assessment work will be specified in the POAMs. (Estimated Completion Date to complete vulnerability correction or mitigation, or to have all POAMs in place, based on receipt of final report: December 31, 2016)

OIG Recommendation: 3.6. Ensure POA&Ms are created to remedy infrastructure vulnerabilities identified in the Dell and Total System Services, Inc., data center environments.

Management Response: The Department concurs with this recommendation. OCIO will work with system owners to remediate findings and/or create a POA&M(s) as required. Any identified infrastructure vulnerability that cannot be resolved by the System Owner will require an approved Risk Acceptance Decision by the Departments Chief Information Security Officer (CISO). In addition, the Department CIO will continue to define the FITARA oversight processes to ensure all IT contracts are properly reviewed prior to award to prevent weak contract language. This activity will be completed by March 31, 2017. (Planned Completion: March 2017)

REPORTING METRIC DOMAIN No. 4: Identity and Access Management

OIG Recommendation: 4.1. Enforce two-factor authentication on all remote connections. (Repeat Recommendation).

Management Response: The Department concurs with this recommendation and has taken great strides during FY 2016 to improve Identity and Access Management. That said, OCIO has made progress during FY 2016 in deploying two-factor authentication to citizen-facing applications. OCIO implemented two-factor authentication for 40,000 users of the G5 citizen-facing information system and has engaged GSA on the possible use of Login.gov for two-factor authentication for other public facing information systems. The Department will continue to work with System Owners to develop a plan to enforce two-factor authentication on the websites and network resources identified in the final report. The plan will specify the milestone schedule and completion dates for when all identified systems will have implemented enforcement of two-factor authentication. This activity will be completed by March 31, 2017. (Planned Completion: March 2017)

OIG Recommendation: 4.2. Create POA&Ms to remedy database vulnerabilities identified in the CAMS, EDSTAR, PAS, and COD environments.

Management Response: The Department concurs with this recommendation and has taken great strides during FY 2016 to improve Identity and Access Management. FSA performed a risk analysis for all Oracle installations located at the Virtual Data Center (VDC). FSA continues to reassess and approve the associated risk on an annual basis. For any database vulnerability outside of the VDC not documented with a current risk acceptance decision, the OCIO will work with system owners to establish a POA&M within 30 days of the issuance of the final report for the identified vulnerability. If the vulnerability cannot be resolved by January 31, 2017, the vulnerably will require an approved Risk Acceptance Form by the Department CISO. This activity will be completed by January 31, 2017. (Planned Completion: January 2017)

OIG Recommendation: 4.3. Resolve access issues to ensure the OIG can complete future vulnerability assessments for the PAS environment.

Management Response: The Department concurs with this recommendation. The Department CIO requests (at minimum) bi-weekly meetings during future audit activities with the OIG audit staff to ensure future issues are raised in a timely manner and receive proper prioritization from all parties. Developing formal and ongoing communication during audit activities will also allow for timely resolution of any identified access issues or critical vulnerabilities.

OIG Recommendation: 4.4. Enforce two-factor authentication for all users (Federal employees, contractors and external business partners) with unprivileged user network accounts that access internal resources.

Management Response: The Department partially concurs with this recommendation and has taken great strides during FY 2016 to improve Identity and Access Management. During FY 2016, the Department established and implemented policy to enforce two-factor authentication on the Departments networks. As of Q4 of FY 2016, the Department is at 96% enforcement of two-factor for unprivileged accounts. To continue progress the Department will develop a plan to address users who authenticate via alternate two-factor technologies outside of PIV. The Department expects to complete the plan by February 28,

2017. The plan will specify the milestones and completion dates to enforce two-factor authentication for all users with unprivileged user network accounts that access internal resources. (Planned Completion: February 2017)

OIG Recommendation: 4.5. Develop a reporting mechanism that allows the Department to maintain consistent reporting of unprivileged user accounts and network authentication statuses.

Management Response: The Department concurs with this recommendation. The Department will document standard operating procedures to ensure consistent reporting of network accounts. The Department expects to complete this activity by February 28, 2017. (Planned Completion: February 2017)

REPORTING METRIC DOMAIN No. 5: Security and Privacy Training

OIG Recommendation: 5.1. Assess of the knowledge, skills, and abilities of individuals with significant security responsibilities.

Management Response: The Department concurs with this recommendation. The Department's CISO will work with the Department's Chief Human Capital Officer (CHCO) to address the workforce development program requirements as outlined in the Office of Management and Budget (OMB) Memorandum M-16-15. The CISO expects to complete this assessment of the current cyber workforce by July 1, 2017. (Planned Completion: July 2017)

OIG Recommendation: 5.2. Develop security training content to close identified gaps identified by the assessments.

Management Response: The Department concurs with this recommendation. The Departments' CISO will work with the Department's Chief Human Capital Officer (CHCO) to address workforce development program requirements as outlined in the Office of Management and Budget (OMB) Memorandum M-16-15. Activities outlined in M-16-15 include developing a common training program for specific categories of cybersecurity professionals, including, but not limited to, those personnel engaged in incident response and penetration testing activities. The CISO expects to complete this activity by the end of FY 2017. (Planned Completion: September 2017)

REPORTING METRIC DOMAIN No. 6: Continuous Monitoring Management

OIG Recommendation: 6.1. Incorporate additional measures to achieve Level 2 status for their ISCM program. In particular, implement a program that (1) assesses the skills, knowledge, and resources needed to effectively implement an ISCM program at both Levels 1 and 2 and (2) defines ISCM stakeholders and their responsibilities and communicate these across the organization. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation and has taken great strides during FY 2016 to improve Continuous Monitoring Management. In FY 2016, the Department met with System Owners to provide guidance and training on the ISCM process. In FY 2016 and moving forward in FY 2017, the Department will address the OIG recommendations and continue its work with the Department of Homeland Security (DHS) in FY 2017 to implement the Continuous Diagnostic and Mitigation (CDM) tools and solutions in order to implement an ISCM program at Levels 1 and 2. (Planned Completion: September 2017)

REPORTING METRIC DOMAIN No. 7: Incident Response

OIG Recommendation: 7.1. Incorporate additional measure to, at a minimum, achieve Level 2 status of the Incident Response program. In particular, (1) assess the skills, knowledge, and resources needed to effectively implement an incident response program and (2) fully implement and enforce incident response capabilities and tools.

Management Response: The Department concurs with this recommendation and has taken great strides during FY 2016 to improve Incident Response. In FY 2016, the Department conducted Incident Response tabletop exercises to document gaps in processes and identify opportunities to improve Incident Response Policy, engaged a case management vendor to integrate and optimize SOC processes, and established daily integrated SOC meetings between the ED SOC and FSA SOC to facilitate coordination of incident response activities. As stated above, the Department CISO will complete the assessment of the current cyber workforce by July 2017. In addition, the Department will publish updated Incident Response Guidance, OCIO-14 and Breach Response Management Handbook and identify requirements for additional Incident Response and forensic resources by March 31, 2017. The remaining work to fully implement and enforce incident response capabilities and tools is planned to be completed by September 2017. (Planned Completion: September 2017)

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

cc: Ted Mitchell
Jason Gray
Dan Galik
James Runcie
Keith Wilson