
The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report For Fiscal Year 2015

FINAL AUDIT REPORT



**ED-OIG/A11P0001
November 13, 2015**

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
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

Dell	Dell Services Federal Government
Department	U.S. Department of Education
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
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SP	Special Publication
SSLv3	Secure Socket Layer, Version 3
TLS	Transport Layer Security
TSYS	Total System Services, Inc.
VDC	Virtual Data Center




UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

November 13, 2015

TO: John B. King, Jr.
Senior Advisor Delegated Duties of Deputy Secretary of Education
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 2015
Control Number ED-OIG/A11P0001

Attached is the subject final audit report that covers the results of our review 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 for fiscal year 2015. 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 (AARTS). The Department's policy requires that you develop a final corrective action plan for our review in the automated system within 30 calendar 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.

400 MARYLAND AVENUE, S.W., WASHINGTON, DC 20202-1510

Promoting the efficiency, effectiveness, and integrity of the Department's programs and operations.

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: Danny A. Harris, PhD, Chief Information Officer, Office of the Chief Information Officer
Keith Wilson, Chief Information Officer, Federal Student Aid
Steve Grewal, Deputy Chief Information Officer, Office of the Chief Information Officer
Linda Wilbanks, PhD, Director, Information Technology Risk Management Group, Federal Student Aid
Cereda Amos, Audit Liaison, Office of the Chief Information Officer
Dawn Dawson, 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

	<u>Page</u>
EXECUTIVE SUMMARY	1
BACKGROUND	3
AUDIT RESULTS	6
CONTINUOUS MONITORING MANAGEMENT.....	7
CONFIGURATION MANAGEMENT	8
IDENTITY AND ACCESS MANAGEMENT	13
INCIDENT RESPONSE AND REPORTING.....	16
RISK MANAGEMENT.....	17
SECURITY TRAINING	19
PLAN OF ACTION AND MILESTONES.....	22
REMOTE ACCESS MANAGEMENT.....	22
CONTINGENCY PLANNING.....	25
CONTRACTOR SYSTEMS.....	27
OTHER MATTERS	28
SOCIAL ENGINEERING TEST	28
OBJECTIVE, SCOPE, AND METHODOLOGY	29
Enclosure 1: CyberScope FISMA Reporting Metrics	33
Enclosure 2: Management Comments	52

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 2015 FISMA reporting metrics for inspectors general prepared by the U.S. Department of Homeland Security Office of Cybersecurity and Communications, Federal Network Resilience Division.

What Was Our Objective?

Our objective was to determine whether the Department and Federal Student Aid's (FSA) overall information technology security programs and practices were generally effective as they relate to Federal information security requirements. To meet the objective, we conducted audit work and additional testing in the 10 cybersecurity areas covered by the Department of Homeland Security FISMA reporting metrics: (1) Continuous Monitoring Management, (2) Configuration Management, (3) Identity and Access Management, (4) Incident Response and Reporting, (5) Risk Management, (6) Security Training, (7) Plan of Action and Milestones, (8) Remote Access Management, (9) Contingency Planning, and (10) Contractor Systems. 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.¹

What We Reviewed

Within each metric area, except for Plan of Action and Milestones, we reviewed information technology controls, policies and procedures, and current processes to determine whether they operated as intended as specified by the Department of Homeland Security. For Plan of Action and Milestones, we did not test implementation of the program. We report our results on each of these metrics, as required, in Enclosure 1.

Based on our work on these metrics, along with additional work we did to test the Department and FSA's program effectiveness in each area, we developed conclusions on the general effectiveness of each metric. For Continuous Monitoring Management, we based our conclusion on the results of our assessment of the maturity of the agency's Information Security Continuous Monitoring program, using the Information Security Continuous Monitoring Maturity Model.

Our additional testing of effectiveness included, but was not limited to, (1) system-level testing for the Configuration Management, Risk Management, and Contingency Planning metrics; (2) vulnerability assessment and penetration testing of the Education Department Utility for Communications, Applications, and Technology Environment; (3) vulnerability assessment and testing of two mainframe environments; (4) identification and reporting of security incidents;

¹ Our determination of effectiveness is based on the definition cited in NIST SP 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations."

(5) verification of training evidence; (6) testing of remote access control settings; and (7) verification of Plan of Action and Milestones tracking and reporting. In addition, we attempted to acquire personal information from employees by using a phishing email; however, the Department's content filtering system successfully blocked the attempt. We summarize results of this exercise in the "Other Matters" section of this report.

What We Found

We found that while the Department and FSA made progress in strengthening its information security programs, weaknesses remained and the Department-wide information systems continued to be vulnerable to security threats. Specifically, we found that the Department was not generally effective in four security areas—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 areas, we also report that improvements are needed in these areas. For the Department and FSA's plan of action and milestones process, we determined that if implemented as intended, it should be effective. We also determined that the Department's identity and access management programs and practices would be generally effective if implemented properly, but that the Department's controls over access to FSA's mainframe environment need improvement. In particular, we identified several key weaknesses that the Department should focus on. For example, in configuration management, we identified six areas for improvement. Most notably, during our vulnerability and penetration testing of the Education Department Utility for Communications, Applications, and Technology Environment, we were able to exploit configuration weaknesses to access the Department's network. Additionally, of significant concern, neither Dell Services Federal Government nor the Office of the Chief Information Officer detected our activity while we were performing the vulnerability assessment and penetration testing. Also, we noted a significant issue related to third-party access to a contractor-operated critical business system. Because the Department relies almost exclusively on contractors to operate the majority of its systems, we feel that all of the individual findings in our report speak generally to the final security area of contractor systems. 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

Our report contains 16 findings, 10 of which are new and 6 of which are repeat findings. We are also making a total of 26 recommendations (16 of which are new and 10 of which are repeat recommendations) to assist the Department and FSA with increasing the effectiveness of their information security program so that it fully complies with all applicable requirements of FISMA, the Office of Management and Budget, and the National Institute of Standards and Technology.

The Department concurred with 23 of the 26 recommendations and partially concurred with the remaining 3 recommendations (recommendations 1.1, 3.1, and 7.2). 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.

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 establishing 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 were previously established by OMB. FISMA specifically mandates that each evaluation under this section shall 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.

Beginning in fiscal year (FY) 2009, OMB required Federal agencies and OIGs to submit FISMA reporting through the OMB Web portal, CyberScope. 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) and plans to extend the maturity model to other security domains for OIGs to utilize in their FY 2016 FISMA reviews. The maturity model is designed to provide perspective on the overall status of information security within an agency, as well as across agencies. It summarizes the status of agency information security programs and their maturity on a 5 level scale.

In February 2015, the U.S. Department of Education (Department) was allocated with a total of \$683 million for their information technology (IT) investments for FY 2015.

In September 2007, the Department entered into a contract with Dell Services Federal Government (Dell) to provide and manage 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 network infrastructure and an enterprise-wide IT environment 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. Under this type of contract, Dell owns all of the wide-area and local-area network devices, routers, switches, external firewalls, network servers, 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 (VDC), which is located at the contractor’s facility in Plano, Texas. The VDC is a general support system utilized by Federal Student Aid (FSA) to consolidate many of its student financial aid program systems to improve interoperability and reduce costs. It serves as the host 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 complex network infrastructure, mainframe computers, a wide array of network servers, and the corresponding operating systems.

Dell is also responsible for the operation of FSA's Common Origination and Disbursement system, a technical solution that schools access to build a high-level student financial aid life cycle for Pell Grant and Direct Loan programs. More specifically, the Common Origination and Disbursement system simplifies the process for schools to obtain financial aid for their students. The system comprises multiple subsystems that span two data centers in Plano, Texas, (which Dell Operates) and Columbus, Georgia, which Total System Services, Inc. (TSYS) operates under a subcontract with Accenture, FSA's prime contractor.

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 and FISMA. OCIO implements the operative principles established by legislation and regulation, establishes a management framework to improve the planning and control of IT investments, and leads change to improve the efficiency and effectiveness of the Department's operations.

AUDIT RESULTS

Based on the requirements specified in FISMA and the FY 2015 U.S. Department of Homeland Security FISMA Inspector General Report Metrics instructions, our audit focused on reviewing 10 areas of the Department's information security program: Continuous Monitoring Management, Configuration Management, Identity and Access Management, Incident Response and Reporting, Risk Management, Security Training, Plan of Action and Milestones (POA&M), Remote Access Management, Contingency Planning, and Contractor Systems.²

We found that the Department was not generally effective in four security areas—Continuous Monitoring, Configuration Management, Incident Response and Reporting, and Remote Access Management. Although we determined that the Department's and FSA's information technology security programs were generally effective in key aspects of three metric areas—Risk Management, Security Training, Contingency Planning—we also report that improvements are needed in these areas. For the Department and FSA's POA&M process, we determined that if implemented as intended, it should be effective. We also determined that the Department's Identity and Access Management programs and practices would be generally effective if implemented properly, but that the Department's controls over access to FSA's mainframe environment need improvement. Our assessments in those nine metric areas reflect our assessment of IT security management in the metric area of Contractor Systems.

The eight metric areas in which we had findings contained repeat findings from the following OIG reports issued from FYs 2011 through 2014:

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

In its response to the draft report, the Department concurred or partially concurred with our findings and recommendations. The comments are summarized at the end of each finding. The full text of the Department's comments to the draft report is included as Enclosure 2 to this report.

² For the area of Continuous Monitoring, the Office of Inspector General was required to assess the maturity level of the program.

CONTINUOUS MONITORING MANAGEMENT

We determined that the overall ISCM program for the Department and FSA was not effective because the program met attributes only for level 1 of the Council of the Inspectors General on Integrity and Efficiency's ISCM maturity model. Level 1 means that their ISCM programs are ad-hoc—not formalized and activities are performed in a reactive manner.³ 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. We also note that the Department and FSA had developed a project plan to address the timely implementation of an ISCM program that meets NIST requirements. The goal of ISCM is to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Until ISCM is fully implemented, the Department and FSA will continue to rely on manual processes. We discuss additional details in the "Risk Management" section of the report.

Issue 1. The Department and FSA's ISCM Program Needs Improvement

The ISCM maturity model provides perspective on the overall status of information security within an agency, as well as across agencies. In this year's FISMA audit, the Department-wide ISCM program was assessed against three categories: (1) people, (2) processes, and (3) technologies.⁴ The Department's and FSA's maturity levels are based on whether they meet all attributes for that level.⁵

We determined that the Department and FSA's ISCM program was at level 1 of the maturity model. Level 1 means that the ISCM program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad hoc program that does not meet requirements for a program with a maturity level of 2. Specifically, we found that the Department and FSA did not meet level 2 requirements because (1) stakeholders' responsibilities had not been effectively communicated across the organization; (2) an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program had not been performed; (3) policies and procedures had not been established to define how ISCM information will be shared with individuals with significant security responsibilities and how these responsibilities would be used to make risk-based decisions; and (4) ISCM results varied depending on who performed the activity, when it was performed, and the methods and tools used.

In accordance with NIST Special Publication (SP) 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," security control effectiveness

³ Under the model, a maturity of level 3 or higher (out of 5 levels) would represent general effectiveness. At level 3, an ISCM program would be characterized as being consistently implemented across the agency.

⁴ Per OMB's updated metrics released in final on June 19, 2015, 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.

⁵ To reach a particular level of maturity, the Department and FSA should meet all attributes outlined in that respective level.

addresses the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment. This is consistent, at a minimum, with level 3 of the maturity model. The Department and FSA were in the process of developing and implementing ISCM policies and procedures that, if implemented correctly, could help the Department in progressing to the next maturity level.

Recommendation

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

- 1.1 Incorporate additional measures to achieve level 2 status for its ISCM program. In particular, ensure that a program is put in place that effectively communicates stakeholders' responsibilities; assesses their skills, knowledge, and resources; clearly defines how ISCM information will be shared with individuals with significant security responsibilities; and consistently applies ISCM results.

Management Comments

The Department partially concurred with the recommendation. OCIO stated that it has assessed the Department's Continuous Monitoring Program at a maturity level 2, in accordance with Department of Homeland Security guidance, and indicated that to address our recommendation, it will reassess the maturity level and ensure that the Department is at a maturity level 2 by the end of FY 2016. Planned completion date is September 2016.

OIG Response

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

CONFIGURATION MANAGEMENT

We determined that the Department's configuration management program was not generally effective because of key weaknesses in application connection protocols; unsupported operating systems in the production environment; interface connections operating on expired certificates; the inability to detect unauthorized devices connecting to the network; and weaknesses in identifying and resolving configuration management vulnerabilities in the EDUCATE environment. These weaknesses are especially concerning because they create vulnerabilities that could potentially expose the Department's systems to allow unauthorized users to gain access to Department systems and resources. However, we found that although some of the policies were outdated, the Department established policies and procedures that were consistent with NIST and that it had processes for maintaining and updating inventories for systems, connections, operating systems, and Web certificates.

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

We determined that Department policies and procedures governing the configuration management program generally incorporated key aspects of NIST guidance, with the exception of the four policies identified under issue 2a. We found that configuration management plans existed and were consistent with NIST guidance. We also found that the Department had processes for maintaining and updating its inventories of systems, connections, operating systems, as well as a list of certificates that identified certificate renewal and expiration dates. However, our work identified weaknesses in the following six areas.

Issue 2a. Configuration Management Policies and Procedures Were Not Current With NIST and Department Guidance (Repeat Finding)

Although the OCIO 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. We determined that of the 24 policies the Department and FSA established for configuration management, the following 4 were outdated (ranging from 3 to 9 years overdue), and did not reflect current requirements:

1. OCIO-11, “Handbook for Information Technology Security Configuration Management Planning Procedures,” 2005;
2. Department’s Standard Operating Procedures, SEC-R009, “Vulnerability Assessment and Risk Remediation,” 2011;
3. OCIO’s, “Information Technology Security Baseline Configuration Guidance,” 2009; and
4. OCIO 1-106, “Administrative Communications System Departmental Directive—Lifecycle Management Framework,” 2010.

NIST SP 800-53, Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations,” 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.⁶ OCIO defines this frequency as annually. OCIO did not update these four configuration management policies and procedures because it had not established a timely internal review and approval process. 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 FISMA audit. 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 current requirements, even when policies had not been updated.

Issue 2b. The Department Was Not Using Appropriate Application Connection Protocol

We found that the Department continued to use outdated secure connection protocols for many of its connections. As part of OIG testing, we judgmentally selected 11 commonly used externally accessible connections out of 1,227 connections in the Department’s inventory for

⁶ 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.

testing. We inspected and validated their protocol settings to ensure they were compliant with current standards and determined that 5 that had a non-secure protocol as an alternative connection protocol.

NIST SP 800-52, Revision 1, “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 shall 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 nonsecure SSLv3 connection to its network and did not take the necessary steps to ensure only recommended secure TLS connections were used. The transition from the SSLv3 to TLS connection would help safeguard users by providing a secure connection. Without this secure connection, users could expose the system to a number of vulnerabilities and exploits, including man-in-the-middle attacks that could jeopardize Department resources.⁷ Given the types of connections at issue, these vulnerabilities have the potential to affect every employee of the Department and a significant number of external users.

Issue 2c. The Department Used Unsupported Operating Systems in Its Production Environment

The Department relied on a number of operating systems on the EDUCATE system that are no longer supported by its vendors. In April 2015, OIG obtained an inventory of 9,669 network accessible interfaces.⁸ From that inventory list, we determined that 962 (about 10 percent) used operating systems that no longer receive vendor support. The Department was unable to provide any documentation, such as Risk Assessment Forms, to justify the use of unsupported systems.

NIST SP 800-53, Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations,” requires organizations to (1) replace information system components when support for the components is no longer available from the developer, vendor, or manufacturer or (2) provide justification and documents approval for the continued use of unsupported system components required to satisfy mission and business needs. Although the Department had policies and procedures to implement this requirement, the Department did not follow them. According to Department officials, they were aware of a number of expired systems that would continue to operate in the EDUCATE environment because they were supporting special applications. However, the officials stated that some application owners submitted corrective action plans to upgrade their respective systems. Because the vendors were no longer supporting the 962 operating systems, no one was addressing new vulnerabilities, leaving the Department’s operating systems at unknown risk.

Issue 2d. The Department Allowed User Interface Connections to Operate on Expired Certificates

The Department allowed remote user Web connections to operate with expired certificates. Certificates allow secure connections from a Web server to a browser. Our review of a listing of

⁷ 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.

⁸ The provided inventory accounted for all systems, including printers, scanners, fax machines, and so on.

all certificates with the certificate renewal and expiration dates showed that two of the Department's major Web connections were not on the list and were operating on expired certificates. When we informed the Department of this, it renewed the certificate for one of the Web connections. For the other, the Department said it was aware that the certificate had expired on January 1, 2015, but would decommission the Web connection on September 30, 2015. On September 30, 2015, the Department notified users that the Web connection would be decommissioned on an unspecified date. However, as of October 19, 2015, the Department has not decommissioned the connection and it was still operating under an expired certificate.

Under NIST SP 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," CM-3, organizations are required to have a process to address the validity of certificates, including expiration. Because the Department did not maintain a complete inventory of certificates, including certificates for two major Web connections, it had no assurance that certificates were kept current. Consequently, the Department was vulnerable to having its connections compromised.

Issue 2e. The Department Was Unable to Detect Unauthorized Devices Connected to Its Network (Repeat Finding)

The Department had no mechanism to restrict the use of unauthorized devices on its network. The Department plans to use a network access control 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. During our FY 2015 FISMA fieldwork, the Department launched and tested the initial phase of the network access control solution that was limited to monitoring its capabilities, but it had not been implemented. According to Department officials, the implementation of the next phase for network access control, which could give the Department the ability to validate or quarantine personal devices before allowing their connection to Department network ability, is scheduled for the first quarter of FY 2016.

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 anti-malware technologies from the organization's secure configuration baseline, such as anti-malware 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 on internal network segments could allow the perpetrators to bypass two-factor authentication, obtain the Department's internet protocol

addresses, and gain access to Department internal resources.⁹ We also identified this condition in our FY 2011 and FY 2014 FISMA audits.

Issue 2f. Controls for Identifying and Resolving Configuration Management Vulnerabilities in the EDUCATE Environment Need Improvement

OCIO's implementation and management of the technical security architecture supporting the EDUCATE general support system need improvements to effectively restrict unauthorized access to the Department's information and resources. We performed a vulnerability assessment of the data center environment and found that some controls were effectively implemented for protecting information resources. However, we identified several areas in which improving the security architecture could further enhance EDUCATE's overall security posture. These included areas such as internal intrusion detection, vulnerability scanning, and patching. Of particular concern, we successfully exploited a vulnerability in one of these areas and used it as a pivot point to gain access to other systems. If an attacker gained similar access either through an external vulnerability or a phishing attack, there is a high likelihood that the EDUCATE system could be compromised.

OCIO did not implement remedial actions to address 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, "Recommended Security Controls for Federal Information Systems and Organizations," SI-2 Flaw Remediation, requires the Department to address any security weakness 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 identified similar conditions during our FY 2011, 2012, and 2013 audit reports. We provided detailed information on the vulnerabilities to OCIO for remediation.

Recommendations

We recommend that the Deputy Secretary require OCIO to—

- 2.1 Ensure that policies and procedures are reviewed and revised at least on an annual basis, or as needed. (Repeat Recommendation)
- 2.2 Update the outdated configuration management policies and procedures to reflect current NIST and industry standards. (Repeat Recommendation)
- 2.3 Immediately establish TLS 1.1 or higher as the only connection for all Department connections.
- 2.4 Discontinue the use of or develop a justification for using unsupported operating systems.

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

- 2.5 Implement procedures to timely replace all operating systems that no longer receive vendor support.
- 2.6 Establish procedures to identify, track, and renew security certificates prior to expiration.
- 2.7 Enable the network access control solution to validate and restrict personal devices from connecting to the Department's internal network. (Repeat Recommendation)
- 2.8 Immediately correct or mitigate the vulnerabilities identified during the vulnerability assessment.

Management Comments

The Department concurred with the recommendations.

OIG Response

In its response, the Department provided a description of actions it has taken, or intends to take, to address our findings and recommendations. We believe that if properly implemented, the actions would be responsive to our finding and recommendations.

IDENTITY AND ACCESS MANAGEMENT

We determined that the Department's identity and access management programs and practices would be generally effective if implemented properly. The Department had adequately designed controls in place for managing user access, however, its controls over access to FSA's mainframe environment needs improvement. For its own employees the Department had policies and procedures consistent with NIST, established a mechanism for tracking and monitoring users, enforced the 90 day password requirement, established a process for granting and terminating user access to its systems and facilities, and implemented two-factor authentication for its systems and applications. The Department is also responsible for overseeing the access to its systems by external users, but in our limited testing of one contractor-operated critical FSA business system we identified major access control issues.

Identity and access management includes the identification, use of credentials, and management of user access to network resources. It also includes the management of the user's physical and logical access to federal facilities and network resources.

Based on our review, we found that the Department established policies and procedures for managing its identity and access management program for its employees that is consistent with NIST standards. Specifically, we determined that the Department established a mechanism for tracking and monitoring internal users of each system. Our testing showed that user activity logs were being maintained and reviewed for two systems, as required. We determined that the Department established a process to track and monitor that employees are adhering to rules of behavior for use of Department systems. We also reviewed the configuration settings and confirmed that the 90 day password requirement password is being enforced. We also validated

the Department's process for granting user access to its systems and facilities was operating in accordance with federal guidance. Additionally, users, including contractors and third parties, are required to use two-factor authentication. We also determined that the Department has a process in place to ensure that employees are granted access based on needs and separation of duties principles, and that user access was terminated and deactivated for employees once no longer required. However, our additional work found that user access controls for FSA's mainframe environment needs improvement.

Issue 3. Access Controls for the FSA's Mainframe Environment Need Improvement

FSA's implementation and management of the technical security architecture supporting the Department's mainframe environments needs improvements to effectively restrict unauthorized access to the Department's information and resources. The OIG performed a vulnerability assessment of two different mainframe environments that process FSA information. We discovered that both the FSA's VDC and TSYS had effectively implemented some controls for protecting information resources on the mainframe. However, several areas were identified with significant deficiencies or where improvements in the security architecture could further enhance the mainframe's overall security posture. In particular, we found accounts for authorized Departmental users with excessive permissions, unauthorized access to data, weak data resource rules, unclear security software privileges, account management weaknesses, and inadequate separation of duties. Detailed information on the vulnerabilities was provided to OCIO and FSA for remediation.

In addition, we found that FSA did not have reasonable assurance that commercial users of a subcontractor-operated mainframe supporting the Common Origination and Disbursement system do not have access to Department data. Specifically, TSYS, the Accenture sub-contractor responsible for the operations of the Common Origination and Disbursement mainframe system, did not provide requested evidence that commercial, non-Department of Education-related, TSYS customers did not have access to Department data. TSYS refused to provide the OIG with documentation reflecting a complete listing of all userids with privileges on the mainframe, which was necessary to evaluate whether those users could improperly access Department data.

TSYS signed a Mainframe Testing Plan agreement in May 2015 that allowed the OIG to acquire all needed information to be analyzed prior to the OIG site visit in July 2015, including a listing of all userids with privileges. However, TSYS failed to provide the required information prior to the site visit and restricted parts of access during the site visit. After repeated requests, TSYS provided on October 1, 2015, a copy of Education userids with privileges, but redacted all other userids with privileges in the mainframe environment. OIG was unable to complete a comprehensive off-site vulnerability assessment of the environment and determine whether other customers on the mainframe could improperly access Department data.

NIST SP 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," provides guidelines and security controls that organizations need to follow regarding system access controls.¹⁰ FSA has not taken the necessary steps to address access requirements needed to protect the integrity of information systems and data. In addition, FSA

¹⁰ Specifically, Account Management (AC-2), Access Enforcement (AC-3), Separation of Duties (AC-5), and Least Privilege (AC-6).

did not implement a process to regularly scan and validate the security of the mainframe or database systems to assure that access rights have been assigned in accordance with federal and agency mandates. Failure to regularly validate the security posture of systems and databases could lead to data leakage and exposure.

Although the mainframe deficiencies are important and should be addressed, the mainframes only represent a small fraction of the computer systems used in the Department's business operations.

Recommendations

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

- 3.1 Immediately correct or mitigate the vulnerabilities identified during the vulnerability assessments.
- 3.2 Direct Accenture to obtain a complete list of userids with privileges from TSYS and produce it to FSA and the OIG; and, in the event of refusal or inability to produce the requested information, take appropriate action under the contract or other authority to ensure that Department data hosted by TSYS on the Common Origination and Disbursement mainframe is adequately safeguarded from unauthorized access.
- 3.3 Determine if non-Departmental users have access in other shared environments that the Department uses in its business environments and take steps to prevent unauthorized access to Departmental data.

Management Comments

The Department partially concurred with recommendation 3.1, and concurred with recommendations 3.2, and 3.3. In response to the recommendation 3.1, FSA stated that it scanned the mainframe and data base systems during December 2014 and January of 2015, and indicated that it plans to scan them again during the same timeframe in FY 2016. Management comments further indicated that FSA performs scans when changes occur, and as part of the Ongoing Security Authorization process. According to FSA, NIST assigned controls are scanned quarterly, annually and tri-annually. Specifically, the Account Management control (AC-2) is scanned annually; Access Enforcement (AC-3) is scanned quarterly; Separation of Duties (AC-5) is scanned tri-annually; and Least Privilege (AC-6) is scanned annually. To fully address the recommendation, FSA will implement CyberArk for least privilege control of privileged users, and, Access Request Management System for account management. This is planned for completion in September 2016.

OIG Response

In its response, the Department provided a description of actions it has taken, or intends to take, to address our finding and recommendations. We believe that if properly implemented, the actions would be responsive to our finding and recommendations.

INCIDENT RESPONSE AND REPORTING

We determined that the Department's overall incident response and reporting program was not generally effective because we identified key weaknesses in its detection and prevention of system penetrations. Specifically, during our testing of the EDUCATE environment, OIG testers were able to gain full access to the Department's network and our access went undetected. However, we found the Department was generally effective at ensuring proper incident response and reporting once incidents are reported, because it had policies and procedures consistent with NIST, and it established a real-time security operations center and had a process for tracking, monitoring, and resolving security incidents.

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.

Based on our review, we found that the Department established policies and procedures for managing its incident response and reporting program consistent with NIST standards. We confirmed that the Department and FSA established a security operations center for responding to, analyzing, and reporting security incidents. Based on our observation and review of the Department's security operations center, we determined that its incident response and reporting process was operating to allow for 24-hour monitoring. We independently verified that the Department tracked and monitored security incidents in a centralized manner in its Operational Vulnerability Management System. For the 137 security incidents reported from October 2014 through February 2015, we randomly selected and analyzed 45 security incidents and verified that all but one of the incidents were reported timely to the U.S. Computer Emergency Readiness Team and law enforcement, as required. We obtained and reviewed four weekly and three monthly incident reports that the Department used as part of its coordination activities. Our review showed that the Department was using this information to identify, track, report, and resolve incidents. However, based on vulnerability assessment testing, we identified a significant vulnerability in the area of detecting and preventing unauthorized access, as discussed below.

Issue 4. Improvements Needed To Detect and Prevent Unauthorized Access

OCIO and Dell's capabilities to detect and prevent unauthorized access need improvement. During our vulnerability assessment testing of the data center that supports the EDUCATE environment, we found that OCIO and Dell did not always have effective mechanisms to prevent, detect, monitor, and report unauthorized access and suspicious activity for the EDUCATE network and systems. Specifically, during our testing of the EDUCATE environment, OIG testers were able not only to gain full access to the Department's network, but also to use this access to pivot from this entry point and launch attacks on other systems connected to the Department, all undetected. The Department's defenses to monitor user activity inside their networks and to prevent such activity did not detect our testers nor terminate their access. As a result, the OIG testers were able to access the Department's network and remained on the network for hours without being detected by either OCIO or Dell. Although the Department's infrastructure had a layered and hardened perimeter, the Department lacked the ability to detect internal or lateral movement once a bad actor gained access to the inside of the infrastructure. Typically, internal suspicious activity or access can be attributed to an actual

insider (employee) attempting to exceed permissions or scanning activity, or through some sort of phishing activity conducted by an external hacker.

NIST SP 800-53, Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations,” requires coordination of incident handling capabilities for unauthorized access across Department components or elements, where the incident handling incorporates preparation, detection and analysis, containment, eradication, and recovery. Controls to protect against unauthorized access failed to alert OCIO and Dell of the possible suspicious activity. The Department’s internal intrusion detection and prevention system, including monitoring for unauthorized access, was not configured effectively; therefore, it failed to detect the unauthorized access on its network and the system owners did not trigger a single alarm. Given the types of systems compromised during our testing, without the proper capabilities to detect unauthorized access and mitigate similar attacks, the Department could face the high risk of a data breach of sensitive personally identifiable information or even the sabotage of the IT infrastructure or critical business systems.

Recommendation

We recommend that the Deputy Secretary require OCIO to—

- 4.1 Ensure the Department’s intrusion detection and prevention system and its technical security architecture are properly configured to restrict and eliminate unauthorized access to Department resources.

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.

RISK MANAGEMENT

We determined that the Department’s risk management program was generally effective because it had established policies and procedures consistent with NIST standards, relied on and used a Department-wide risk management framework, established a risk methodology to assess its systems, and established an inventory of relevant documentation needed to assess system risk. However, the Department needs to take steps to ensure that it timely conducts system security authorizations.

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.

Based on our review, we found that the Department established policies and procedures for governing its risk management program consistent with NIST standards. We found that the Department relied on and used the Risk Management Framework to govern its risk management program.¹¹ Phases of the Risk Management Framework include (1) categorizing the systems, (2) identifying and tailoring security controls, (3) implementing security controls, (4) assessing security controls, (5) authorizing systems, and (6) continuously monitoring systems. As part of the Risk Management Framework, the Department assigned risk based on a risk scoring methodology. We confirmed the use of this methodology by attending a risk scoring session where we noted that OCIO and system owners designed strategies to remediate vulnerabilities as part of their risk approach. We obtained and analyzed documents relevant to the risk management program, such as security authorizations, security assessments, and authorizations to operate, and determined that despite discrepancies identified below, the Department generally met the intent of the risk management program.

Issue 5. OCIO's System Authorization Process Needs Improvement (Repeat Finding)

OCIO's system authorization process needs improvement. We identified several deficiencies in system security plans, authorization to operate documents, security assessment reports, and expired system authorizations (formerly called certification and accreditation).

On February 23, 2015, the Department reported a total of 184 systems in its inventory.¹² Of the 184 systems, we found 33 systems (18 percent) with expired or missing information. We note, however, that 25 of the 33 systems with expired documentation were categorized as low risk, and the remaining 8 were moderate. Specifically, from the 184 systems, we found

- 26 (14 percent) were operating on expired security authorizations,¹³
- 21 (11 percent) were operating on expired control self-assessments, and
- 21 (11 percent) were operating on expired contingency plans.

¹¹ The Risk Management Framework is a high-level phased approach implementation strategy that identifies objectives, principles, and activities to be considered when integrating cybersecurity risk management into organizational processes and the systems development life cycle. Although the Department has developed and is following the process that makes up the framework, the policy for framework is currently going through the final approval process.

¹² In February 2015, the Department inventory of FISMA reportable systems in the Operational Vulnerability Management Solution accounted for 234 systems.

Later that month, the Department underwent major clean-up efforts of the Operational Vulnerability Management System and as a result, the inventory of FISMA reportable systems was reduced to 184. Therefore, for the purpose of Risk Management testing, we relied on 184 systems.

¹³ The security authorization process involves an official management decision to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, staff, and other organizations based on the implementation of an agreed-on set of security controls.

For a more in-depth review of the system authorization process for the Department's risk management program, we judgmentally selected 14 of the 184 systems. Of the 14 systems, we found

- 1 system was listed on the inventory at a lower Federal Information Processing Standards Publication 199 system categorization level than it was authorized for, and then was reflected in its system security plan;
- 1 system operated with an expired authorization to operate; and
- 1 system did not have an authorization to operate decision letter.

NIST SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems," requires security authorization packages to contain the security plan, the security assessment report, and a POA&M. Authorizing officials use the information in these key documents to make risk-based authorization decisions. Unless an agency has implemented continuous monitoring, it must reauthorize its systems every 3 years to continue operation. Providing orderly, disciplined, and timely updates to the security plan, security assessment report, and corrective action plans supports the concept of near real-time risk management and ongoing authorization.

Although NIST SP 800-37, Revision 1, emphasizes the importance of maintaining up-to-date security authorization packages for systems authorized to operate, and the Department had the policies and procedures to implement the NIST requirements, it did not follow them. This resulted in ineffective and inconsistent certifying and accrediting of systems within the required 3-year timeframe, allowing system authorizations to expire. Because the Department was not implementing a timely security authorization process, it operated with unknown security risks for those systems with expired documentation.

Recommendation

We recommend that the Deputy Secretary require OCIO to—

- 5.1 Develop a process to ensure that policies and procedures for authorizing systems are followed. (Repeat Recommendation)

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 TRAINING

We determined that the Department had a generally effective security training program because it had established policies and procedures consistent with NIST standards, a comprehensive training program, and a mechanism for tracking the status of security training activities. We

found that the Department was adequately identifying and tracking the security awareness training status for a total of 4,207 employees. However, we identified a relatively minor issue related to the documentation of new employee 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.

Based on our review, we found that the Department established policy and procedures for managing its security awareness training program consistent with NIST standards. We examined the Department's training program and found that it included appropriate IT security content for the organization. We reviewed the actual content approved for the training and found that it contained key IT security concerns. We obtained a listing of all Department users required to take security training by August 2015 and found that the Department identified and tracked the status of security awareness training for its employees. We determined that the Department has the capability to meet its program obligations relating to security training. However, we identified an area of improvement relating to the Department's ability to document its security awareness training. Although we identified an area of improvement below, we determined that the Department satisfied the overall metric.

Issue 6. Documentation Not Complete Supporting New User IT Security Awareness Training Before New Users Accessed Network

The Department did not provide documentation to support that new users received IT security awareness training before they obtained access to its network. According to OCIO officials, new employees are required to review a PowerPoint presentation prior to the first day of employment.¹⁴ After reviewing the PowerPoint presentation, the employee is required to print and sign a form acknowledging completion of the training. The signed certificate of completion is then provided to Department officials at the employee's orientation session on the first day of employment before gaining access to the Department's IT systems. In addition, after the first day of employment, new employees are required to take the official annual Cyber Security and Privacy Awareness Training within 10 working days of employment.

We identified 118 new users from October 2014 through March 2015. We judgmentally selected the 35 most recently hired employees who began employment between January and February 2015 and asked OCIO to provide us with support that security awareness training was completed before the employees were granted access to the network. The Department was unable to provide documentation to support that the 35 new employees completed IT security awareness training. Further inquiry disclosed that, due to weather conditions, the new employee orientation was never conducted and no make-up session was offered. In addition, 10 of the 35 employees completed the Department's annual Cyber Security and Privacy Awareness Training

¹⁴ The title of the PowerPoint presentation is "New Employee Introduction to Cyber Security and Privacy Awareness."

after the required 10 business days of employment, as mandated by OCIO policy, without consequence; while the remaining 25 did complete the training within the required 10 business days.

OMB Circular A-130, Appendix III, “Security of Federal Automated Information Resources,” requires that agencies must ensure that all staff are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. NIST SP 800-50 “Building an Information Technology Security Awareness and Training Program,” Section 1.5.2, requires chief information officers to ensure that effective tracking and reporting mechanisms for security training are in place. In addition, according to the OCIO-01, “Handbook for Information Assurance/Cybersecurity Policy,” one of the key responsibilities of Information System Security Officers is to ensure that system users understand their cybersecurity responsibilities by tracking user completion of Department security training and awareness.

The Department did not have procedures to obtain documentation to support that new employees completed security awareness training when the Department canceled new employee orientation. In addition, the Department did not have a process that effectively ensured that all new employees completed the Cyber Security and Privacy Awareness training within the required 10 business days of employment. All users of the Department’s automated information systems must be able to apply the concepts of the IT security policies and be able to take appropriate steps to avert IT security situations. For the Department’s IT program to be successful, each user of the Department’s IT resources needs to assume responsibility for IT security. We also identified this condition in our FY 2012 and 2013 FISMA audits.

Recommendations

We recommend that the Deputy Secretary require OCIO to—

- 6.1 Ensure that it has documentation to support that all new users complete security awareness training prior to accessing the Department’s network or any Department information systems.
- 6.2 Establish procedures to track all new employees to ensure that they complete the Cyber Security and Privacy Awareness training within 10 days of employment.
- 6.3 Establish procedures to suspend user access when an employee has failed to complete the Cyber Security and Privacy Awareness training within 10 days of employment.

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.

PLAN OF ACTION AND MILESTONES

We determined that the Department and FSA's POA&M policies and procedures were consistent with NIST, contained a process for identifying and tracking IT security weaknesses, and established a centralized process that operated to track and remediate all active POA&Ms. Therefore, if implemented as intended, they should be effective. However, we did not test implementation of the POA&M program to be able to conclude effectiveness.

A POA&M, also referred to as a corrective action plan, is a management tool for tracking the mitigation of cyber security program and system-level findings and weaknesses. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. 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.

Based on our review, we found that the Department and FSA established policies and procedures for managing IT security weaknesses consistent with NIST standards. We found that the Department and FSA used POA&Ms to identify and track IT security weaknesses. To track the status of POA&M remediation, the Department and FSA use a centralized tracking system called the Operational Vulnerability Management System. From the Operational Vulnerability Management System, we obtained and reviewed a list of 1,587 POA&Ms created by the Department and FSA that were identified between October 2014 and May 2015. This list identified each POA&M according to threat description, threat level, and assigned with an estimated and actual completion date for each system. We concluded that the Department had a process to track, prioritize, and assign for remediation of all active POA&Ms according to policies and procedures.

REMOTE ACCESS MANAGEMENT

We determined that the Department's remote access management program was not generally effective because it did not enforce its network time-out requirement or, more significantly, use two-factor authentication for two of its network connections. In particular, we found that two network connections only required a username and password to connect to Departmental resources. Although the Department had established policies and procedures consistent with NIST, as well as a process to manage mobile devices, we found that the severity and impact of not enforcing two-factor authentication on these particular network connections could result in a potential compromise of Departmental 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 computer 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.

Based on our review, we found that the Department established policies and procedures for managing its remote access management program consistent with NIST standards. We obtained and analyzed various secure network connection methods the Department used for key solutions, such as email, and determined that these network connections worked as intended. We analyzed

all mobile device management solutions the Department used and found that they also worked as intended. We confirmed that the Department had a process for performing security impact analysis for its mobile devices. We tested and verified that the Department enabled two-factor authentication for Outlook Web Access, a key vulnerability we previously identified.¹⁵ We also confirmed that FSA discontinued using Social Security numbers as identifiers for user accounts in response to our prior recommendations. However, we did identify significant weaknesses with enforcing the time-out requirement for remote access connections, and two-factor authentication.

Issue 7a. The Department Did Not Consistently Enforce the Remote Access Time-Out Requirement

The Department did not consistently comply with the 30-minute time-out of user inactivity for remote connections as OMB mandates. Specifically, we found that the Department failed to enforce this requirement on its virtual private network connection for remote users. We found that users were able to remain inactive for as long as 120 minutes before the session timed out. Initially, Department officials stated that this requirement had been implemented and all Department connections were configured to time out after 30 minutes of inactivity. When we communicated the results of our test to the Department, it acknowledged that further testing was needed and would work to resolve this deficiency.

OMB 07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” requires the use of a time-out function after 30 minutes of inactivity for remote access and mobile devices. The Department did not effectively test and verify the inactivity setting to ensure that it worked correctly. Without this setting, a user (especially one logged into a third-party location) could expose the Department’s networks and compromise the confidentiality, integrity, and availability of information and information systems. We identified similar conditions in our FY 2011 and 2012 FISMA audits, which the Department subsequently resolved for the identified connections. However, the FY 2015 audit identified other remote connections that the Department had not corrected when it remediated the other connections.

Issue 7b. Two External Network Connections Did Not Use Two-Factor Authentication (Repeat Finding)

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 remote connections used by the Department. The Department identified four remote connections. To verify the number of remote connections on the Department’s network, we conducted targeted scans that identified two additional remote connections that provided users with the ability to remotely connect to FSA’s internal network without using two-factor authentication. The OIG notified the Department of this discrepancy and the Department subsequently confirmed that the two additional remote connections we identified were valid and should have been included as part of the remote connections inventory. We accessed six remote connections and found that the two connections that we identified were not configured to use two-factor authentication. These remote connections were configured to connect to Department resources using one-factor

¹⁵ Outlook Web Access provides users remote access to their work email.

authentication that was limited to a username and a password, and were not included in the list provided to us by the Department. Furthermore, after being notified of these connections, the Department did not disable these network connections, or enable two-factor authentication.

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, “Security and Privacy Controls for Federal Information Systems and Organizations,” requires the use of two or more different 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 failed to enforce the use of two-factor identification for its remote connections because the Department was not aware that two additional remote solutions were operational on its network. 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 cyber attacks. Also, not requiring external users to use two-factor authentication places the systems and the data at risk for exposure from unauthorized users. Because the Department was unaware of remote connections that were operational on its network, it did not ensure that remote access complied with OMB requirements for two-factor authentication to strengthen the assurance of the user’s identity. We identified similar conditions in our FY 2011, 2012, 2013, and 2014 FISMA audits.

Recommendations

We recommend that the Deputy Secretary require OCIO to—

- 7.1 Validate the inactivity settings to ensure sessions are timing out after 30 minutes of inactivity.
- 7.2 Enforce two-factor authentication on all remote connections. (Repeat Recommendation).
- 7.3 Establish an accurate inventory of all remote connections.

Management Comments

The Department concurred with the recommendations 7.1, and 7.3, and partially concurred with recommendation 7.2. In its response to recommendation 7.2, FSA stated that it has already applied two-factor authentication to the remote connections noted in our review. FSA also indicated that it has implemented CyberArk for least privilege control of all privileged users in its VDC, and for its systems outside of the VDC, the implementation of Personal Identity Verification – Interoperable (or PIV-I) is scheduled to be completed by the end of 2015.

OIG Response

In its response, the Department provided a description of actions it has taken, or intends to take, to address our finding and recommendations. We believe that if properly implemented, the actions would be responsive to our finding and recommendations. For the two-factor

authentication to the remote connections identified in our review, OIG will perform a verification as part of its FY 2016 FISMA review.

CONTINGENCY PLANNING

We determined that the Department and FSA had a generally effective contingency planning program because it had established policies and procedures consistent with NIST, a comprehensive disaster recovery process, and a centralized repository for storing and tracking Department and FSA contingency plans and testing results. However, we found documentation issues regarding the completeness of contingency plans and business impact analyses.

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

Based on our review, we found that the Department established policies and procedures for its contingency planning program consistent with NIST standards. We determined that the Department and FSA have established an annual process to plan, execute, and document disaster recovery test results. During FY 2013 and FY 2014, the OIG observed two disaster recovery exercises conducted for two key general support systems—VDC and EDUCATE. In both exercises, FSA and the Department successfully tested and recovered its operations.¹⁶ In FY 2015, we attended and observed disaster recovery readiness and status meetings and verified that outstanding issues were assigned for remediation. For 14 Departmental and FSA systems, we verified that the contingency plans were centrally stored and tracked in Operational Vulnerability Management System. For these 14 systems, we obtained and analyzed IT security contingency plans and testing results and determined that the Department and FSA generally met the intent of the contingency planning program. However, we did identify the following areas where the Department and FSA can improve the documentation of its contingency plans and testing.

Issue 8a. Information System Contingency Plans Were Not Complete (Repeat Finding)

The Department and FSA did not always document the IT recovery procedures for its systems in accordance with NIST guidelines and Departmental policies. We judgmentally selected 14 contingency plans for review. Of the 14 plans reviewed, we found that 9 did not include all the required information system contingency planning elements identified in NIST guidelines and Departmental guidance.¹⁷ Specifically, we found that some of the contingency plans did not contain documentation for (1) the roles and responsibilities of key individuals and function; (2) key individual's contact information in the event of a disaster; (3) training requirements; (4) an alternate storage site for system backups; (5) backup procedures to include the frequency of backups and offsite storage instructions; (6) an alternate processing site, when required; (7) planned testing, exercise, and maintenance activities; or (8) alternate telecommunication services, when required. Although contingency plans were established, certain elements of the

¹⁶ The disaster recovery exercise is an activity crucial to restore operability following a major disruption and is a key component of this program.

¹⁷ NIST SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems," May 2010; and OCIO-10 "Handbook for Information Technology Security Contingency Planning Procedures."

plans were either missing, or incomplete.

According to NIST SP 800-34, Revision 1, information system contingency plan development is a critical step in the process of implementing a comprehensive contingency planning program. A proper plan contains detailed roles, responsibilities, teams, and procedures associated with restoring an information system following a disruption. We also identified this condition in our FY 2012, 2013, and 2014 FISMA audits.

Issue 8b. Business Impact Analysis Process Needs Improvement

OCIO did not consistently document a Business Impact Analysis (BIA) for its systems in accordance with NIST guidelines and Departmental procedures.¹⁸ Specifically, 3 of 14 of systems' contingency plans we reviewed lacked supporting documentation to validate the completion of a BIA. The BIA enables the Information System Contingency Plan Coordinator to characterize the system components, supported mission/business processes, and interdependencies. This assists the Information System Contingency Plan Coordinator to determine contingency planning requirements and priorities. OCIO did not ensure that the Information System Security Officers and system owners were documenting a BIA as part of the development of their contingency plans. Complete documentation of a BIA will allow the Department to sufficiently identify and prioritize information systems and components critical to supporting the Department's mission and business functions. We also identified this condition in our FY 2012 FISMA audit.

Issue 8c. Information System Contingency Plan Testing Process Needs Improvement (Repeat Finding)

OCIO and FSA did not have documentation to support that the testing of systems' contingency plans had been performed in accordance with NIST and Departmental guidance. For 6 of the 14 systems reviewed, we did not find documentation to support that contingency plan testing was performed and documented on an annual basis, as required. Department officials did not require the Information Systems Security Officers or system owners to document results of contingency plan tests for its systems and, therefore, we could not determine if testing actually occurred.

NIST SP 800-34 Revision 1, "Contingency Planning Guide for Federal Information Systems," states that testing is a critical element of a viable contingency capability and enables plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan. OCIO-10, "Handbook for Contingency Planning Procedures," states, it is important that the Management Team conducts training and plan testing at least annually. This will ensure the effectiveness of the contingency plan and allow the recovery teams to gain practical experience in coordinating their activities and working together. Without complete documentation of contingency plan testing, the Department and FSA might not be aware of critical element deficiencies affecting its systems that need to be corrected and included for future contingency plan testing. We also identified this condition in our FY 2012 and 2014 FISMA audits.

¹⁸ NIST SP 800-34, Revision 1, and OCIO-10, "Handbook for Information Technology Security Contingency Planning Procedures," July 12, 2005.

Recommendations

We recommend that the Deputy Secretary and the Under Secretary require OCIO and FSA, respectively, to:

- 8.1 Review and update system contingency plans for the nine systems that have elements missing to ensure that all the required contingency planning elements are included, as required by NIST guidance. (Repeat Recommendation)
- 8.2 Review and update system contingency plans for all remaining Department and FSA systems to ensure that all required contingency planning elements are included, as required by NIST guidance. (Repeat Recommendation)
- 8.3 Ensure that Business Impact Analyses for the three OCIO systems identified are documented.
- 8.4 Review all remaining OCIO and FSA systems to ensure a BIA has been conducted and is documented. (Repeat Recommendation)
- 8.5 Document contingency plan test results for the six systems in question as required by NIST guidelines and Departmental procedures. (Repeat Recommendation)
- 8.6 Review and document contingency plan tests for all remaining Department and FSA systems. (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 findings and recommendations.

CONTRACTOR SYSTEMS

Because the Department relies almost exclusively on contractors to operate its systems, we are not making a separate conclusion on the effectiveness of the Department's program to oversee the security of contractor systems. Our assessment of all of the prior FISMA aspects of IT security management included in this report implicitly addresses issues of contractor oversight. As of February 2015, the Department's system inventory identified 127 contractor-operated systems. According to OCIO, whether the systems are contractor-operated or agency-operated, all Department systems reported in the inventory are required to meet the security requirements that FISMA, OMB, and NIST set forth. Because the Department operates in an environment in which most of its systems are contractor-operated, the Department needs to ensure that it provides sufficient oversight to remediate the system related weaknesses identified throughout our report wherever they involve contractors.

OTHER MATTERS

SOCIAL ENGINEERING TEST

As part of this year's audit, we performed a high-level phishing attempt to determine Department employees' security awareness in recognizing cyber threats that may potentially compromise the Department's network and resources, including disclosure of personally identifiable information. The Department's content filtering system successfully blocked the phishing links and warned users about the testing team's suspected phishing attempts, so the testing team's phishing emails did not reach recipients.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of our audit 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 the FY 2015, Inspector General, Federal Information Security Modernization Act Reporting Metrics, we not only assessed the expected level of performance for 10 security metric areas, but also performed additional testing to formulate our conclusion on the overall effectiveness of the Department-wide program and operations for 8 of the 10 areas. For Plan of Action and Milestones we did not test implementation of the program to conclude its effectiveness, and for Contractor Systems our assessment of all of the prior FISMA aspects of IT security management included in this report implicitly addresses issues of contractor oversight. The required security metric areas were (1) Continuous Monitoring Management, (2) Configuration Management, (3) Identity and Access Management, (4) Incident Response and Reporting, (5) Risk Management, (6) Security Training, (7) Plan of Action and Milestones, (8) Remote Access Management, (9) Contingency Planning, and (10) Contractor Systems. For FY 2015, Offices of Inspectors General were also required to evaluate the maturity level of the Continuous Monitoring Management metric.

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 2015 Inspector General FISMA reporting metrics;
- compared and tested management, operational, and technical controls based on NIST standards and Department guidance; and
- assessed the Department's progress in correcting information security weaknesses identified in prior OIG audit reports by reviewing information from the Audit Accountability and Resolution Tracking System to identify and evaluate the corrective action plans for implementing each of the recommendations made from FY 2011 through FY 2014.¹⁹

To assess effectiveness, we performed the following:

- performed system-level testing for the Configuration Management, Risk Management and Contingency Planning metrics;
- performed vulnerability assessment and penetration testing of EDUCATE;

¹⁹ The Audit Accountability and Resolution Tracking System is a Web-based application that assists the Department's audit reporting and follow-up.

- conducted vulnerability assessment and testing of mainframe environments;
- analyzed security incidents;
- verified training evidence and completion;
- verified credentials within the access management; and
- verified security settings for the Department data protection.

In addition, we attempted a social engineering exercise to test employees' security awareness. Results of this exercise are summarized in the "Other Matters" section of this report

As of February 2015, the Department identified an inventory of 234 FISMA-reportable IT systems.²⁰ Out of the 234 FISMA reportable systems we concentrated on 136 systems that were classified as high and moderate. We judgmentally selected 16 of the Department's IT systems to ascertain the security control aspects relating to Configuration Management, Risk Management, and Contingency Planning.²¹ The 16 systems selected included 1 mission critical system from the judgmental sample selected as part of our FY 2014 FISMA audit. We selected this system to measure progress from the prior fiscal year. We judgmentally selected the remaining 15 systems based on Department principal offices with a high and medium concentration levels of systems relative to the inventory of 136 Department systems.²² As we began our fieldwork, we learned that two of the systems selected from the inventory that we were provided were not active systems. Specifically, the Electronic Records Management System had expired and was no longer an active system. In addition, we learned that the Integrated Technical Architecture was not a system, but part of the General Support System/VDC's shared environment infrastructure. Therefore, our judgmental sample size was reduced to 14.

The table below lists the systems selected, the system's principal office, and the Federal Information Processing Standards Publication 199 potential impact level.²³

Number	System Name	Principal Office	Impact Level
1	Common Origination and Disbursement Electronic Notes	FSA	MODERATE
2	Integrated Student Experience	FSA	MODERATE
3	Operational Vulnerability Management Solution	FSA	MODERATE
4	Student Loan Collection System	FSA	MODERATE
5	Education Central Automated Processing System	OCIO	MODERATE
6	EDUCATE Messaging	OCIO	MODERATE
7	I3 Community of Practice and Public Information	OII*	MODERATE

²⁰ Later, in February, the Department provided a revised inventory of 184 systems; however, we had already completed our sample selection process. See footnote 12 for further details.

²¹ 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.

²² The OIG was removed from the universe of systems because we typically review the OIG every 2 years. We reviewed OIG systems as part of the FY 2014 FISMA audit.

²³ FIPS 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.

	System		
8	Promise Neighborhood Website System	OII	MODERATE
9	EDFacts	OPEPD*	MODERATE
10	Budget Service Budget Formulation	OPEPD	MODERATE
11	Accreditation and State Liaison	OPE*	MODERATE
12	Jacob K. Javits Fellows Database	OPE	MODERATE
13	TRIM Trio	OSERS*	MODERATE
14	Department of ED/Perkins	OCTAE* (formerly OVAE*)	MODERATE

* Office of Innovation and Improvement (OII); Office of Planning, Evaluation and Policy Development (OPEPD); Office of Postsecondary Education (OPE); Office of Special Education and Rehabilitative Services (OSERS); Office of Vocational and Adult Education (OVAE); Office of Career, Technical, and Adult Education.

In addition to the sample of 14 systems, we obtained a separate universe of newly hired Department employees that began employment from October 1, 2014, through March 2015. We chose to exclude certain categories of new hires from this list (for example, transfer and non-career employees), and arrived at a population of 118 employees. Out of the 118 employees, we judgmentally selected 35 newly hired employees from the most recent 2 months to ascertain the security control aspect relating to the Security Training metric. Those 35 employees represented newly hired Department employees who began employment from January 1, 2015, through February 28, 2015.²⁴ Furthermore, to accommodate our testing for the Remote Access Management metric, we relied on the Department-provided inventory of 1,227 connections and judgmentally selected 11 externally accessible connections that were commonly used. Finally, for incident response and reporting, we selected a nonstatistical random sample of 45 out of 137 incidents that occurred between October 1, 2014 and February 28, 2015. Because we relied on nonstatistical sampling approaches, the results of our sampling cannot be projected to the audit universe.

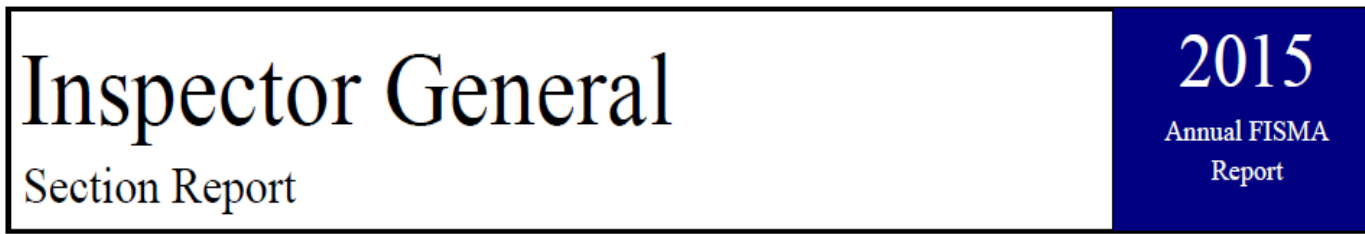
For this audit, we reviewed the security controls and configuration settings for EDUCATE, the VDC, and multiple major applications. We used computer-processed data for the Configuration Management, Identity and Access Management, Incident Response and Reporting, Risk Management, Security Training, and Remote Access Management metrics to support the findings summarized in this report. We also performed an assessment of the computer-processed data and determined this data was 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. Each 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. Since we did not perform specific testing to determine the effectiveness of Identity and Access Management, and POA&M, our assessment of the data for these metric areas was limited to assessing the controls for the overall process. We conducted our fieldwork from January 2015 through September 2015, primarily at

²⁴ Because we did not select a statistically random sample, any results found during our analysis were not projected across the entire population of newly hired Department employees.

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 September 21, 2015, and again on October 29, 2015, to discuss details pertaining to the draft report that were not discussed in the previous meeting.

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.

Enclosure 1: CyberScope FISMA Reporting Metrics



Department of Education

Section 1: Continuous Monitoring Management

- 1.1 Utilizing the ISCM maturity model definitions, please assess the maturity of the organization's ISCM program along the domains of people, processes, and technology. Provide a maturity level for each of these domains as well as for the ISCM program overall.

- 1.1.1 Please provide the D/A ISCM maturity level for the People domain.

Ad Hoc (Level 1)

Comments:

"The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report For Fiscal Year 2015," Audit Control Number ED-OIG/A11P0001, hereafter referred to as FISMA Report.
Issue 1. The Department and FSA's ISCM Program Needs Improvement.

- 1.1.2 Please provide the D/A ISCM maturity level for the Processes domain.

Ad Hoc (Level 1)

Comments:

"The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report For Fiscal Year 2015," Audit Control Number ED-OIG/A11P0001, hereafter referred to as FISMA Report.
Issue 1. The Department and FSA's ISCM Program Needs Improvement.

- 1.1.3 Please provide the D/A ISCM maturity level for the Technology domain

Defined (Level 2)

Comments:

"The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report For Fiscal Year 2015," Audit Control Number ED-OIG/A11P0001, hereafter referred to as FISMA Report.
Issue 1. The Department and FSA's ISCM Program Needs Improvement.

- 1.1.4 Please provide the D/A ISCM maturity level for the ISCM Program Overall.

Ad Hoc (Level 1)

Comments:

"The U.S. Department of Education's Federal Information Security Modernization Act of 2014 Report For Fiscal Year 2015," Audit Control Number ED-OIG/A11P0001, hereafter referred to as FISMA Report.
Issue 1. The Department and FSA's ISCM Program Needs Improvement.

- 1.2 Please provide any additional information on the effectiveness of the organization's Information Security Continuous Monitoring Management Program that was not noted in the maturity model above.

Not used.

Section 2: Configuration Management

Section 2: Configuration Management

- 2.1 Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

No

Comments: We determined that the Department's configuration management program was not generally effective because of key weaknesses in application connection protocols; unsupported operating systems in the production environment; interface connections operating on expired certificates; the inability to detect unauthorized devices connecting to the network; and weaknesses in identifying and resolving configuration management vulnerabilities in the EDUCATE environment.

- 2.1.1 Documented policies and procedures for configuration management.

No

Comments: FISMA Report: Issue 2a. Configuration Management Policies and Procedures Were Not Current With NIST and Department Guidance (Modified Repeat Finding)

- 2.1.2 Defined standard baseline configurations.

Yes

Comments: No exceptions noted.

- 2.1.3 Assessments of compliance with baseline configurations.

Yes

Comments: No exceptions noted.

- 2.1.4 Process for timely (as specified in organization policy or standards) remediation of scan result findings.

Yes

Comments: No exceptions noted.

- 2.1.5 For Windows-based components, USGCB secure configuration settings are fully implemented (when available), and any deviations from USGCB baseline settings are fully documented.

Yes

Comments: No exceptions noted.

Section 2: Configuration Management

2.1.6 Documented proposed or actual changes to hardware and software baseline configurations.

No

Comments: FISMA Report: Issue 2c. The Department Used Unsupported Operating Systems in Its Production Environment

2.1.7 Implemented software assessing (scanning) capabilities (NIST SP 800-53: RA-5, SI- 2).

No

Comments: FISMA Report: Issue 2b. The Department Was Not Using Appropriate Application Connection Protocol

2.1.8 Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards. (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2).

Yes

Comments: No exceptions noted.

2.1.9 Patch management process is fully developed, as specified in organization policy or standards, including timely and secure installation of software patches (NIST SP 800-53: CM-3, SI-2).

Yes

Comments: No exceptions noted.

2.2 Please provide any additional information on the effectiveness of the organization's Configuration Management Program that was not noted in the questions above.

See Narrative for Exceptions Noted.

Comments: FISMA Report:
Issue 2d. The Department Allowed User Interface Connections to Operate on Expired Certificates.
Issue 2e. The Department Was Unable to Detect Unauthorized Devices Connected to Its Network (Modified Repeat Finding).
Issue 2f. Controls for Identifying and Resolving Configuration Management Vulnerabilities in the EDUCATE Environment Need Improvement (Modified Repeat Finding)

2.3 Does the organization have an enterprise deviation handling process and is it integrated with an automated scanning capability?

Yes

Comments: No exceptions noted.

Section 2: Configuration Management

- 2.3.1 Is there a process for mitigating the risk introduced by those deviations? A deviation is an authorized departure from an approved configuration. As such it is not remediated but may require compensating controls to be implemented.

Yes

Comments: No exceptions noted.

Section 3: Identity and Access Management

- 3.1 Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and which identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes?

Yes

Comments: We determined that the Department's identity and access management programs and practices would be generally effective if implemented properly.

- 3.1.1 Documented policies and procedures for account and identity management (NIST SP 800-53: AC-1).

Yes

Comments: No exceptions noted.

- 3.1.2 Identifies all users, including Federal employees, contractors, and others who access organization systems (HSPD 12, NIST SP 800-53, AC-2).

Yes

Comments: No exceptions noted.

- 3.1.3 Organization has planned for implementation of PIV for logical 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).

Yes

Comments: No exceptions noted.

- 3.1.4 Organization has planned for implementation of 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).

Yes

Comments: No exceptions noted.

Section 3: Identity and Access Management

3.1.5 Ensures that the users are granted access based on needs and separation-of-duties principles.

Yes

Comments: No exceptions noted.

3.1.6 Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. IP phones, faxes, printers).

Yes

Comments: No exceptions noted.

3.1.7 Ensures that accounts are terminated or deactivated once access is no longer required according to organizational policy.

Yes

Comments: No exceptions noted.

3.1.8 Identifies and controls use of shared accounts.

Yes

Comments: No exceptions noted.

3.2 Please provide any additional information on the effectiveness of the organization's Identity and Access Management Program that was not noted in the questions above.

See Narrative for Exceptions Noted.

Comments: FISMA Report: Issue 3. Access Controls for the FSA's Mainframe Environment Need Improvement

Section 4: Incident Response and Reporting

4.1 Has the organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

No

Comments: We determined that the Department's overall incident response and reporting program was not generally effective because we identified key weaknesses in its detection and prevention of system penetrations.

Section 4: Incident Response and Reporting

- 4.1.1 Documented policies and procedures for detecting, responding to, and reporting incidents (NIST SP 800-53: IR-1).

Yes

Comments: No exceptions noted.

- 4.1.2 Comprehensive analysis, validation, and documentation of incidents.

Yes

Comments: No exceptions noted.

- 4.1.3 When applicable, reports to US-CERT within established timeframes (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).

Yes

Comments: No exceptions noted.

- 4.1.4 When applicable, reports to law enforcement and the agency Inspector General within established timeframes.

Yes

Comments: No exceptions noted.

- 4.1.5 Responds to and resolves incidents in a timely manner, as specified in organization policy or standards, to minimize further damage (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).

Yes

Comments: No exceptions noted.

- 4.1.6 Is capable of correlating incidents.

Yes

Comments: No exceptions noted.

- 4.1.7 Has sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).

No

Comments: FISMA Report: Issue 4. Improvements Needed To Detect and Prevent Unauthorized Access

Section 4: Incident Response and Reporting

- 4.2 Please provide any additional information on the effectiveness of the organization's Incident Management Program that was not noted in the questions above.

Not used.

Section 5: Risk Management

- 5.1 Has the organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

Comments: We determined that the Department's risk management program was generally effective because it had established policies and procedures consistent with NIST standards, relied on and used a Department-wide risk management framework, established a risk methodology to assess its systems, and established an inventory of relevant documentation needed to assess system risk.

- 5.1.1 Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1.

Yes

Comments: No exceptions noted.

- 5.1.2 Addresses risk from a mission and business process perspective and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800-37, Rev. 1.

Yes

Comments: No exceptions noted.

- 5.1.3 Addresses risk from an information system perspective and is guided by the risk decisions from an organizational perspective and the mission and business perspective, as described in NIST SP 800-37, Rev.1.

Yes

Comments: No exceptions noted.

- 5.1.4 Has an up-to-date system inventory.

No

Comments: FISMA Report: Issue 5. OCIO's System Authorization Process Needs Improvement (Modified Repeat Finding)

Section 5: Risk Management

5.1.5 Categorizes information systems in accordance with government policies.

Yes

Comments: No exceptions noted.

5.1.6 Selects an appropriately tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.

Yes

Comments: No exceptions noted.

5.1.7 Implements the approved set of tailored baseline security controls specified in metric 5.1.6.

Yes

Comments: No exceptions noted.

5.1.8 Assesses the security 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.

Yes

Comments: No exceptions noted.

5.1.9 Authorizes information system operation 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.

Yes

Comments: No exceptions noted.

5.1.10 Information-system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization.

Yes

Comments: No exceptions noted.

5.1.11 Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO).

Yes

Comments: No exceptions noted.

Section 5: Risk Management

- 5.1.12 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.

Yes

Comments: No exceptions noted.

- 5.1.13 Security authorization package contains system security plan, security assessment report, POA&M, accreditation boundaries in accordance with government policies for organization information systems (NIST SP 800-18, 800-37).

Yes

Comments: No exceptions noted.

- 5.1.14 The organization has an accurate and complete inventory of their cloud systems, including identification of FedRAMP approval status.

Yes

Comments: No exceptions noted.

- 5.1.15 For cloud systems, the organization can identify the security controls, procedures, policies, contracts, and service level agreements (SLA) in place to track the performance of the Cloud Service Provider (CSP) and manage the risks of Federal program and personal data stored on cloud systems.

Yes

Comments: No exceptions noted.

- 5.2 Please provide any additional information on the effectiveness of the organization's Risk Management Program that was not noted in the questions above.

Not used.

Section 6: Security Training

Section 6: Security Training

- 6.1 Has the organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

Comments: We determined that the Department had a generally effective security training program because it had established policies and procedures consistent with NIST standards, a comprehensive training program, and a mechanism for tracking the status of security training activities.

- 6.1.1 Documented policies and procedures for security awareness training (NIST SP 800-53: AT-1).

Yes

Comments: No exceptions noted.

- 6.1.2 Documented policies and procedures for specialized training for users with significant information security responsibilities.

Yes

Comments: No exceptions noted.

- 6.1.3 Security training content based on the organization and roles, as specified in organization policy or standards.

Yes

Comments: No exceptions noted.

- 6.1.4 Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other organization users) with access privileges that require security awareness training.

No

Comments: FISMA Report: Issue 6. Documentation Not Complete Supporting New User IT Security Awareness Training Before New Users Accessed Network (Modified Repeat Finding)

- 6.1.5 Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training.

Yes

Comments: No exceptions noted.

Section 6: Security Training

6.1.6 Training material for security awareness training contains appropriate content for the organization (NIST SP 800-50, 800-53).

Yes

Comments: No exceptions noted.

6.2 Please provide any additional information on the effectiveness of the organization's Security Training Program that was not noted in the questions above.

Not used.

Section 7: Plan Of Action & Milestones (POA&M)

7.1 Has the organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

Comments: We determined that the Department and FSA's POA&M policies and procedures were consistent with NIST, contained a process for identifying and tracking IT security weaknesses, and established a centralized process that operated to track and remediate all active POA&Ms. Therefore, if implemented as intended, they should be effective.

7.1.1 Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation.

Yes

Comments: No exceptions noted.

7.1.2 Tracks, prioritizes, and remediates weaknesses.

Yes

Comments: No exceptions noted.

7.1.3 Ensures remediation plans are effective for correcting weaknesses.

Yes

Comments: No exceptions noted.

Section 7: Plan Of Action & Milestones (POA&M)

7.1.4 Establishes and adheres to milestone remediation dates and provides adequate justification for missed remediation dates.

Yes

Comments: No exceptions noted.

7.1.5 Ensures resources and ownership are provided for correcting weaknesses.

Yes

Comments: No exceptions noted.

7.1.6 POA&Ms include security weaknesses discovered during assessments of security controls and that require remediation (do not need to include security weakness due to a risk- based decision to not implement a security control) (OMB M-04-25).

Yes

Comments: No exceptions noted.

7.1.7 Costs associated with remediating weaknesses are identified in terms of dollars (NIST SP 800-53: PM-3; OMB M-04-25).

Yes

Comments: No exceptions noted.

7.1.8 Program officials report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53:CA-5; OMB M-04-25).

Yes

Comments: No exceptions noted.

7.2 Please provide any additional information on the effectiveness of the organization's POA&M Program that was not noted in the questions above.

Not used.

Section 8: Remote Access Management

Section 8: Remote Access Management

- 8.1 Has the organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

No

Comments: We determined that the Department's remote access management program was not generally effective because it did not enforce its network time-out requirement or use two-factor authentication for two of its network connections.

- 8.1.1 Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST SP 800-53: AC-1, AC-17).

Yes

Comments: No exceptions noted.

- 8.1.2 Protects against unauthorized connections or subversion of authorized connections.

Yes

Comments: No exceptions noted.

- 8.1.3 Users are uniquely identified and authenticated for all access (NIST SP 800-46, Section 4.2, Section 5.1).

No

Comments: FISMA Report: Issue 2e. The Department Was Unable to Detect Unauthorized Devices Connected to Its Network (Modified Repeat Finding)

- 8.1.4 Telecommuting policy is fully developed (NIST SP 800-46, Section 5.1).

Yes

Comments: No exceptions noted.

- 8.1.5 Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms.

No

Comments: FISMA Report: Issue 7b. Two External Network Connections Did Not Use Two-Factor Authentication

- 8.1.6 Defines and implements encryption requirements for information transmitted across public networks.

Yes

Comments: No exceptions noted.

Section 8: Remote Access Management

- 8.1.7 Remote access sessions, in accordance with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required.

No

Comments: FISMA Report: Issue 7a. The Department Did Not Consistently Enforce the Remote Access Time-Out Requirement (Modified Repeat Finding)

- 8.1.8 Lost or stolen devices are disabled and appropriately reported (NIST SP 800-46, Section 4.3; US-CERT Incident Reporting Guidelines).

Yes

Comments: No exceptions noted.

- 8.1.9 Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4).

Yes

Comments: No exceptions noted.

- 8.1.10 Remote-access user agreements are adequate in accordance with government policies (NIST SP 800-46, Section 5.1; NIST SP 800-53, PS-6).

Yes

Comments: No exceptions noted.

- 8.2 Please provide any additional information on the effectiveness of the organization's Remote Access Management that was not noted in the questions above.

Not used.

- 8.3 Does the organization have a policy to detect and remove unauthorized (rogue) connections?

Yes

Comments: No exceptions noted.

Section 9: Contingency Planning

Section 9: Contingency Planning

- 9.1 Has the organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

Comments: We determined that the Department and FSA had a generally effective contingency planning program because they had established policies and procedures consistent with NIST, a comprehensive disaster recovery process, and a centralized repository for storing and tracking Department and FSA contingency plans and testing results.

- 9.1.1 Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST SP 800-53: CP-1).

Yes

Comments: No exceptions noted.

- 9.1.2 The organization has incorporated the results of its system's Business Impact Analysis and Business Process Analysis into the appropriate analysis and strategy development efforts for the organization's Continuity of Operations Plan, Business Continuity Plan, and Disaster Recovery Plan (NIST SP 800-34).

No

Comments: FISMA Report: Issue 8b. Business Impact Analysis Process Needs Improvement (Modified Repeat Finding)

- 9.1.3 Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures (NIST SP 800-34).

No

Comments: FISMA Report: Issue 8a. Information System Contingency Plans Were Not Complete (Modified Repeat Finding)

- 9.1.4 Testing of system-specific contingency plans.

No

Comments: FISMA Report: Issue 8c. Information System Contingency Plan Testing Process Needs Improvement (Modified Repeat Finding)

- 9.1.5 The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34).

Yes

Comments: No exceptions noted.

Section 9: Contingency Planning

9.1.6 Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53).

No

Comments: FISMA Report: Issue 8a. Information System Contingency Plans Were Not Complete (Modified Repeat Finding)

9.1.7 Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans.

Yes

Comments: No exceptions noted.

9.1.8 After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34).

Yes

Comments: No exceptions noted.

9.1.9 Alternate processing sites are not subject to the same risks as primary sites. Organization contingency planning program identifies alternate processing sites for systems that require them (FCD1, NIST SP 800-34, NIST SP 800-53).

No

Comments: FISMA Report: Issue 8a. Information System Contingency Plans Were Not Complete (Modified Repeat Finding)

9.1.10 Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).

Yes

Comments: No exceptions noted.

9.1.11 Contingency planning that considers supply chain threats.

Yes

Comments: No exceptions noted.

9.2 Please provide any additional information on the effectiveness of the organization's Contingency Planning Program that was not noted in the questions above.

Not used.

Section 10: Contractor Systems

Section 10: Contractor Systems

- 10.1 Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including for organization systems and services residing in a cloud external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

N/A

Comments: Because the Department relies almost exclusively on contractors to operate its systems, we are not making a separate conclusion on the effectiveness of the Department's program to oversee the security of contractor systems.

- 10.1.1 Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities (including other government agencies), including organization systems and services residing in a public, hybrid, or private cloud.

Yes

Comments: No exceptions noted.

- 10.1.2 The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and compliant with FISMA requirements, OMB policy, and applicable NIST guidelines (NIST SP 800-53: CA-2).

Yes

Comments: No exceptions noted.

- 10.1.3 A complete inventory of systems operated on the organization's behalf by contractors or other entities, (including other government agencies), including organization systems and services residing in public, hybrid, or private cloud.

Yes

Comments: No exceptions noted.

- 10.1.4 The inventory identifies interfaces between these systems and organization- operated systems (NIST SP 800-53: PM-5).

Yes

Comments: No exceptions noted.

- 10.1.5 The organization requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.

Yes

Comments: No exceptions noted.

Section 10: Contractor Systems

10.1.6 The inventory of contractor systems is updated at least annually.

Yes

Comments: No exceptions noted.

10.2 Please provide any additional information on the effectiveness of the organization's Contractor Systems Program that was not noted in the questions above.
Not used.

Enclosure 2: Management Comments



UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF THE CHIEF INFORMATION OFFICER

MEMORANDUM

DATE: November 12, 2015

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

FROM: John B. King, Jr. *[Signature]*
Senior Advisor Delegated Duties of Deputy Secretary of Education
Office of the Deputy Secretary

Ted Mitchell *[Signature]*
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 2015
Control Number ED-OIG/A11P0001

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) 2015, Control Number ED-OIG/A11P0001. 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 collaborating and the sharing of mutual goals and objectives.

In FY 2015, OIG's FISMA Audit objective changed from measuring compliance to determining whether the Department's overall information technology security programs and practices were generally effective as they relate to Federal information security requirements. The Department notes that in previous OIG FISMA audits, OIG recommendations were broken down into three separate categories: "New Findings," "Repeat Findings," and "Modified Repeat Findings," where Modified Repeat Findings may have indicated progress by the Department in resolving the repeat finding. However, this category no longer appears in the report.

The Department had made progress in strengthening its information security program, with five of ten reporting metrics noted as generally effective, although repeat weaknesses were still noted in three of five reporting metrics: Risk Management (Repeat Finding);

ED-MARYLAND-001-NEW-NOVEMBER 12, 2015
www.ed.gov

Our mission is to ensure equal access to education and opportunity for all students, regardless of their background or the location of the school.

Security Training (Repeat Finding); Contingency Planning (Repeat Finding); Identity and Access Management; and, Plan of Action and Milestones (POA&M). No conclusion was made for the Contractor Systems metric as assessment of this area is reflected in all other metrics. The Department was not generally effective in the remaining four metrics to include: Configuration Management; Continuous Monitoring; Remote Access; and, Incident Response and Reporting.

In FY 2015, the Department continued its efforts to improve security through several major security implementations and improvements in response to previous audit recommendations. Federal Student Aid (FSA) implemented a new student identification system, Person Authentication Services (PAS), as part of FSA's Enterprise Identity Management Program. PAS addressed significant vulnerabilities in the previous FSA Personal Identification Number (PIN) system, specifically the elimination of the use of social security numbers and a PIN for user identification. The Department implemented a new Security Operations Management (SecOps) system to support the 24x7, on premise Security Operations Center (EDSOC). The SecOps system provides an integrated system to allow joint management of incident response among the various components of the Department including FSA, as well as overall case management and Security Operations Center (SOC) operations. Finally, the Department completed the implementation of the core Continuous Monitoring technologies that enable Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Phase 1 capabilities focused on hardware and software management, asset management, vulnerability management, and configuration management.

The Department has also garnered significant benefits from previous years' audits and expects that the recommendations presented in this audit will further improve the effectiveness of the information security program by strengthening the associated management, technical, and operational security controls. Each finding and recommendation will be addressed as stipulated in the plan provided, and as agreed upon by your office.

The following responses address each recommendation:

REPORTING METRIC No. 1: Continuous Monitoring

OIG Recommendation: 1.1. Incorporate additional measures to achieve level 2 status for the Department's Information Security Continuous Monitoring (ISCM) program. In particular, ensure that a program is put in place that effectively communicates stakeholders' responsibilities; assesses their skills, knowledge, and resources; clearly defines how ISCM information will be shared with individuals with significant security responsibilities; and consistently applies ISCM results.

Management Response: The Department partially concurs with this recommendation. The Office of the Chief Information Officer (OCIO) has assessed the Department's Continuous Monitoring Program at a maturity level 2 status in accordance with DHS guidance. We will reassess the maturity level and ensure that we are at maturity level 2 by the end of FY 2016. (Planned Completion: September 2016).

REPORTING METRIC No. 2: Configuration Management

OIG Recommendation: 2.1. Ensure that policies and procedures are reviewed and revised at least on an annual basis, or as needed. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. OCIO will review the current 'Information Assurance/Cyber Security Document Development, Review and Approval Process' document to ensure that the process defined is efficient and effective and update the document as needed to ensure that policies and procedures are reviewed and revised according to the process. (Planned Completion: February 2016).

OIG Recommendation: 2.2. 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 review current configuration policies, guidance, and procedures, identify gaps and deficiencies, and update the documents to reflect current NIST and industry standards. (Planned Completion: June 2016).

OIG Recommendation: 2.3. Immediately establish TLS 1.1 or higher as the only connection for all Department connections.

Management Response: The Department concurs with this recommendation. FSA has corrective action plans created to discontinue the use of SSLv3 in seven (7) systems. (Planned Completion: January 2016). OCIO will establish TLS 1.1 or higher upon completion of a risk assessment of impacted systems that cannot support TLS 1.1 or higher as previous attempts to implement TLS 1.1 resulted in some system failures. (Planned Completion: January 2016). OCIO will support the development of POA&Ms with respective system owners outside the EDUCATE boundaries.

OIG Recommendation: 2.4. Discontinue the use of or develop a justification for using unsupported operating systems.

Management Response: The Department concurs with this recommendation. OCIO is actively engaged in discontinuing the use of or developing justification for using unsupported operating systems inside the EDUCATE boundaries. (Planned Completion: September 2016). OCIO will also coordinate activities with respective system owners outside of the EDUCATE boundaries.

OIG Recommendation: 2.5. Implement procedures to timely replace all operating systems that no longer receive vendor support.

Management Response: The Department concurs with this recommendation. OCIO will develop procedures to timely identify and replace, or develop justification for, unsupported operating systems. (Planned Completion: March 2016).

OIG Recommendation: 2.6. Establish procedures to identify, track, and renew security certificates prior to expiration.

Management Response: The Department concurs with this recommendation. OCIO will establish procedures to identify, track, and renew security certificates. (Planned Completion: March 2016).

OIG Recommendation: 2.7. 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. OCIO will complete the implementation of the network access control (NAC) solution and enable a policy within NAC to validate and restrict personal devices from directly connecting to the Department's internal network. (Planned Completion: February 2016).

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

Management Response: The Department concurs with this recommendation. OCIO- ITS will re-evaluate current procedures to address vulnerabilities in coordination with OCIO- IAS and EDSOC. (Planned Completion: March 2016).

REPORTING METRIC No. 3: Identity and Access Management

OIG Recommendation: 3.1. Immediately correct or mitigate the vulnerabilities identified during the vulnerability assessments.

Management Response: FSA partially concurs with this recommendation. FSA scanned the mainframe and data base systems December 2014 – January 2015, and will scan again in FY 2016 during the same timeframe. FSA also scans when changes occur and as part of the Ongoing Security Authorization process; specifically: Account Management (AC-2)- Annually; Access Enforcement (AC-3) – Quarterly; Separation of Duties (AC-5) – Tri-annually; and Least Privilege (AC-6) – Annually. FSA will also implement the following applications: CyberArk for least privilege control of Privileged users (Completed 10/30/2015 for internal users); and, Access Request Management System (ARMS) for account management (Planned Completion: September 2016).

OIG Recommendation: 3.2. Direct Accenture to obtain a complete list of userids with privileges from TSYS and produce it to FSA and the OIG; and, in the event of refusal or inability to produce the requested information, take appropriate action under the contract or other authority to ensure that Department data hosted by TSYS on the Common Origination and Disbursement mainframe is adequately safeguarded from unauthorized access.

Management Response: FSA concurs with this recommendation. FSA will work with contracting to require TSYS to produce the complete list of users with privileges. FSA will then provide this information to the OIG. This will be an official requirement that if TSYS refuses, contractual actions can be taken. (Planned Completion: June 2016).

OIG Recommendation: 3.3. Determine if non-Departmental users have access in other shared environments that the Department uses in its business environments and take steps to prevent unauthorized access to Departmental data.

Management Response: FSA concurs with this recommendation. FSA will work with the ISSOs of all systems to identify if non-Departmental users have access in other shared environments that the Department uses in its business environments. FSA will follow Department policies to prevent unauthorized access to Departmental data. (Planned Completion: March 2016).

REPORTING METRIC No. 4: Incident Response and Reporting

OIG Recommendation: 4.1. Ensure the Department's intrusion detection and prevention system and its technical security architecture are properly configured to restrict and eliminate unauthorized access to Department resources.

Management Response: The Department concurs with this recommendation. OCIO will ensure, and validate, that the various service providers are properly configuring and monitoring the intrusion detection/prevention systems supporting the Department's networks. Additionally, a review of the EDUCATE and VDC network security architectures and a gap assessment will be conducted. (Planned Completion: May 2016).

REPORTING METRIC No. 5: Risk Management

OIG Recommendation: 5.1. Develop a process to ensure that policies and procedures for authorizing systems are followed. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. OCIO will complete the migration from the current Operational Vulnerability Management Solution (OVMS) system to the Department of Justice Cyber Security Assessment and Management (CSAM) solution. This migration will provide automation that can help to streamline the assessment and authorization process and potentially free up resources to perform additional security assessments. The CSAM solution will also provide capabilities to assist system stakeholders with the development and maintenance of system security plans. (Planned Completion: January 2016). OCIO will also evaluate and identify the resource requirements to centralize responsibilities for maintaining system status information, such as ATO date and posting of final ATO documentation, in CSAM to ensure that this information is current at all times. (Planned completion: March 2016).

REPORTING METRIC No. 6: Security Training

OIG Recommendation: 6.1. Ensure that it has documentation to support that all new users complete security awareness training prior to accessing the Department's network or any Department information systems.

Management Response: The Department concurs with the recommendation: OCIO will provide instructions to Office of Management (OM) regarding new employees completing Cyber Security and Privacy Awareness (CSPA) Training prior to gaining access to the network. OCIO will work with supervisors to ensure that new employees complete the mandated training within 10 days of employment and notify system owners of new employees who are not compliant with the training requirement. (Planned Completion: January 2016).

OIG Recommendation: 6.2. Establish procedures to track all new employees to ensure that they complete the Cyber Security and Privacy Awareness training within 10 days of employment.

Management Response: The Department concurs with this recommendation. OCIO will establish procedures to track new employees and ensure that they complete the CSPA training in the required timeframe. OCIO will establish procedures and collect documentation showing that required CSPA training has been completed by all new employees and contractors. (Planned Completion: January 2016).

OIG Recommendation: 6.3. Establish procedures to suspend user access when an employee has failed to complete the Cyber Security and Privacy Awareness training within 10 days of employment.

Management Response: The Department concurs with this recommendation. OCIO will establish procedures to track new employees and ensure that they complete the CSPA training by the required timeframe. OCIO will notify system owners of employees who are not compliant with the requirement. The system owners will be required to suspend users from the Department network until the training is completed. (Planned Completion: January 2016).

REPORTING METRIC No. 7: Remote Access Management

OIG Recommendation: 7.1. Validate the inactivity settings to ensure sessions are timing out after 30 minutes of inactivity.

Management Response: The Department concurs with this recommendation. OCIO is taking immediate steps to resolve this issue. (Planned Completion: December 2015).

OIG Recommendation: 7.2. Enforce two-factor authentication on all remote connections. (Repeat Recommendation)

Management Response: FSA partially concurs with this recommendation. FSA has already applied two-factor authentication to the remote connections noted in the review. Additionally, FSA has implemented CyberArk for least privilege control of all privileged users in its Virtual Data Center (VDC), completed October 30, 2015. The FSA systems outside the VDC are scheduled to complete implementation of PIV-I by 2015 year-end. (Planned Completion: December 2015).

OIG Recommendation: 7.3. Establish an accurate inventory of all remote connections.

Management Response: The Department concurs with this recommendation. OCIO will immediately ensure through the EARB governance process that all future remote access connections requested establish and support two-factor authentication. Subsequently, two-factor authentication is a change management requirement prior to production approval via the Change Advisory Board (CAB) process. (Planned Completion: February 2015).

REPORTING METRIC No. 8: Contingency Planning

OIG Recommendation: 8.1. Review and update system contingency plans for the nine systems that have elements missing to ensure that all the required contingency planning elements are included, as required by NIST guidance. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. OCIO will initiate a POA&M, if one does not exist, for each of the nine systems identified as having elements missing to ensure that all required elements are updated within 30 days of POA&M initiation. (Planned creation date for POA&M(s): December 2015).

OIG Recommendation: 8.2. Review and update system contingency plans for all remaining Department and FSA systems to ensure that all required contingency planning elements are included, as required by NIST guidance. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. OCIO and FSA will review system contingency plans for any system that is currently scheduled for an assessment in FY 16 to ensure that all required contingency planning elements are included as required by NIST guidance and issue findings against the system as appropriate. (Planned Completion: September 2016).

OIG Recommendation: 8.3. Ensure that Business Impact Analyses (BIA) for the three OCIO systems identified are documented.

Management Response: The Department concurs with this recommendation. If a POA&M does not already exist, OCIO will initiate one against each of the three systems that were identified as not completing a BIA to ensure that a BIA is completed within 30 days of POA&M initiation. (Planned creation date for POA&M(s): December 2015).

OIG Recommendation: 8.4. Review all remaining OCIO and FSA systems to ensure a BIA has been conducted and is documented. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. OCIO and FSA will review BIAs for any system that is currently scheduled for an assessment in FY 2016 to ensure that BIAs are conducted and appropriately documented. (Planned Completion: September 2016).

OIG Recommendation: 8.5. Document contingency plan test results for the six systems in question as required by NIST guidelines and Departmental procedures. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. If a POA&M does not already exist, OCIO will initiate one against each of the six systems that were identified as not performing and documenting contingency plan test results to ensure that the contingency plan tests are performed and document within 90 days of POA&M initiation. (Planned creation date for POA&M(s): December 2015).

OIG Recommendation: 8.6. Review and document contingency plan tests for all remaining Department and FSA systems. (Repeat Recommendation)

Management Response: The Department concurs with this recommendation. OCIO will re-iterate to Department information system stakeholders the requirement for annual contingency plan tests in accordance with Department policy. (Planned Completion: December 2016).

Thank you for the opportunity to comment on this report and for your continued support of the Department and its critical mission. If you have any questions regarding this matter, please contact Chief Information Officer Danny Harris at (202) 245-6259.

cc: Danny Harris
James Runcie
Keith Wilson
Steve Grewal