The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014

FINAL AUDIT REPORT

This report has been reviewed for public dissemination by the Office of Counsel to the Inspector General. Information requiring protection from public dissemination has been redacted from this report in accordance with the Freedom of Information Act, 5 U.S.C. § 552.

ED-OIG/A11O0001
November 2014

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

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

NOTICE

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

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

Abbreviations/Acronyms Used in this Report

Dell	Dell Services Federal Government
Department	U.S. Department of Education
DHS	Department of Homeland Security
EDUCATE	Education Department Utility for Communications, Applications, and Technology Environment
FISMA	Federal Information Security Management Act of 2002
FSA	Federal Student Aid
FY	Fiscal Year
GFE	Government-Furnished Equipment
IT	Information Technology
NAC	Network Access Control
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
OVMS	Operational Vulnerability Management Solution
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
SP	Special Publication
SSN	Social Security Number
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
USDA	United States Department of Agriculture
VDC	Virtual Data Center

UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

INFORMATION TECHNOLOGY AUDIT DIVISION

November 12, 2014

Memorandum

TO: James H. Shelton, III
Deputy Secretary
Office of the Deputy Secretary

Ted Mitchell
Under Secretary
Office of the Under Secretary

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

SUBJECT: Final Audit Report
Audit of the U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014
Control Number ED-OIG/A11O0001

Attached is the subject final audit report that covers the results of our review of the U.S. Department of Education's (Department) compliance with the Federal Information Security Management Act of 2002 for fiscal year 2014. An electronic copy has been provided to your Audit Liaison Officers. We received your comments on the findings and recommendations in our draft report.

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

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

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

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

Enclosure

Cc: Danny A. Harris, PhD, Chief Information Officer, Office of the Chief Information Officer
Jerry E. Williams, Chief Information Officer, Federal Student Aid
Steve Grewal, Director, Information Assurance Services, Office of the Chief Information Officer
Linda Wilbanks, PhD, Director, Information Technology Risk Management Group, Federal Student Aid
Michael Massino, Policy and Planning Branch Chief, 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
Charles Laster, Post Audit Group, Office of the Chief Financial Officer
L'Wanda Rosemond, AARTS Administrator, Office of Inspector General

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report constitutes the Office of Inspector General's (OIG) independent evaluation of the U.S. Department of Education's (Department) information technology security program and practices, as required by the Federal Information Security Management Act of 2002 (FISMA). OIG's review was based on questions and reporting metrics that the Department of Homeland Security (DHS) provided for the annual FISMA review. The objective of our audit was to determine whether the Department and Federal Student Aid's (FSA) overall information technology (IT) security program and practices were in compliance with the E-Government Act of 2002 (Public Law 107-347), including Title III—Information Security, and related information security standards identified within Office of Management and Budget guidelines. In addition, during the course of our review of the Department's actions to address previous recommendations, we became aware of issues involving the implementation of corrective action plans. Consequently, we assessed the implementation of corrective action plans by the Office of Chief Information Officer and Federal Student Aid.

Based on the FY 2014 FISMA reporting metrics provided by DHS, we assessed the status of the Department's information security posture for fiscal year (FY) 2014. The reporting metrics included Continuous Monitoring, Configuration Management, Identity and Access Management, Incident Response and Reporting, Risk Management, Security Training, Plan of Actions and Milestones, Remote Access Management, Contingency Planning, Contractor Systems, and Security Capital Planning. In addition to the reporting metrics, we also assessed the Department's (1) information security policy and procedures, (2) enterprise-level information security controls, (3) management of information security weaknesses, and (4) system-level security controls.[1] Further, we evaluated the IT processes, policies, and procedures that the Department had already documented, implemented, and monitored.

In addition, the OIG evaluated Department systems, contractor systems, annual self-assessments, policies, procedures, various OIG audit reports, and other Federal agency reports issued throughout the year. We also conducted vulnerability and penetration (both internal and external) testing of a major FSA system located in Columbus, Georgia. The results of the testing are summarized in the body of this report. We also observed the Department's annual disaster recovery exercise conducted in June 2014 at the Department's recovery site in Florence, Kentucky. Furthermore, in a collaborative effort with the United States Department of Agriculture OIG and other Federal OIGs, we volunteered to participate in the agency-wide Council of the Inspectors General on Integrity and Efficiency cloud computing initiative. The results of this review are summarized in the "Other Matters" section of this report.

We determined that the Department's and FSA's IT security program generally complied with the E-Government Act of 2002 (Public Law 107-347), including Title III—Information Security, and related information security standards identified within Office of Management and Budget guidelines. We found that the Department was compliant with the Continuous Monitoring,

[1] For purposes of this audit, enterprise-level security controls are controls that are expected to be implemented.

Security Training, POA&M, Contractor Systems, and Security Capital Planning reporting metrics. Specifically, the Department has established compliant programs for enterprise-wide continuous monitoring, security awareness training, tracking and monitoring known information security weaknesses, overseeing systems operated on its behalf by contractors or other entities, and security capital planning and investments, that are consistent with FISMA requirements, Office of Management and Budget policy, and applicable National Institute of Standards and Technology guidelines.

While the Department made progress in strengthening its information security program, many longstanding weaknesses remain and the Department's information systems continue to be vulnerable to serious security threats. We identified findings in 6 of the 11 reporting metrics. The findings were comprised of repeat or modified repeat findings from OIG reports issued from FYs 2011 through 2013.[2] In addition, we have a new finding regarding the implementation of corrective actions to address some of our previous recommendations. Further, we answered the questions in the U.S. Department of Homeland Security's metrics template based on our audit work, which will become the CyberScope FISMA Report as shown in Enclosure 1.

We also found that: (1) the Department has not remediated outstanding issues from previous OIG audit reports and our work showed that 5 of the 11 reporting metrics contained repeat or modified repeat findings from reports issued from FY 2011 through 2013; and (2) in some instances, although the Department said it has completed a recommendation, we continue to find that the corrective actions were not implemented and we had to issue modified repeat recommendations because the exact or similar conditions continue to exist.

In the areas where we have repeat or modified repeat findings, where the Department continues to implement corrective actions, we are not making additional recommendations. However, we are making 13 new recommendations in areas where we have new findings. Additionally, we are making 7 modified repeat recommendations to address repeat findings in areas where the Department has completed previous corrective actions, but where we have repeat or modified repeat findings. Implementing these new and modified recommendations will assist the Department in establishing and sustaining an effective information security program—one that complies with requirements of FISMA, Office of Management and Budget, and National Institute of Standards and Technology requirements.

The Department's systems contain or protect large amounts of confidential information (personal records, financial information, and other personally identifiable information (PII)) and perform vital organizational functions. Unauthorized individuals might target the systems by exploitation, but trusted individuals inside the Department and Department contractors could also target the systems. Without adequate management, operational, and technical security controls, the Department's systems and information are vulnerable to attacks. Such attacks could lead to a loss of confidentiality resulting from unauthorized access to data. Also, there is increased risk that unauthorized activities or excessive use of system resources could reduce the reliability and integrity of Department systems and its data and increased risk that sensitive data may be released, used, or modified.

[2] Repeat findings are current report findings with the same or similar conditions to those contained in prior OIG reports. A modified repeat finding is identified when a similar finding condition exists; however, the factors that constitute the condition are different.

The Department concurred with 16 of the 20 recommendations and partially concurred with the remaining 4 recommendations (3.1, 3.2, 4.1, and 4.2). 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 (FISMA), permanently reauthorized the framework established by the Government Information Security Reform Act of 2000, which expired in November 2002. FISMA 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. FISMA 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. OMB is responsible for establishing and overseeing policies, standards, and guidelines for information security, and has the authority to approve agencies' information security programs. OMB is also responsible for submitting the annual FISMA report to Congress, developing and approving the cybersecurity portions of the President's Budget, and for the budgetary and fiscal oversight of the agencies' use of funds.

Each agency must establish a risk-based information security program that ensures information security is practiced throughout the lifecycle of each agency's system. 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 addition to the responsibilities listed above, FISMA requires each agency to have an annual independent evaluation of its information security program and practices, including control testing and a compliance assessment. These evaluations are to be performed by the agency's Inspector General or an independent evaluator, and the results of these evaluations are to be reported to OMB. For fiscal year (FY) 2014 reporting, each Inspector General was required by

the Department of Homeland Security to evaluate its respective agency on the following 11 reporting metrics: 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; Contractor Systems; and Security Capital Planning. Beginning in FY 2009, OMB required Federal agencies to submit FISMA reporting through the OMB Web portal, CyberScope.

As of July 2014, the Department had spent a total of $683 million on information technology (IT) investments for FY 2014. The Department budgeted $32.3 million for FY 2014 on IT security and FISMA compliance costs, which equates to 4.7 percent of total IT spending.

In September 2007, the Department entered into a contract with Dell Services Federal Government[3] (Dell) to provide and manage all 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 total IT platform and infrastructure to support Department employees in meeting the Department's mission. The contract was awarded as a 10-year, performance-based, indefinite-delivery, indefinite-quantity contract with fixed unit prices. Under this type of contract, Dell owns all of the IT hardware and operating systems to include wide-area and local-area network devices, network servers, routers, switches, external firewalls, voice mail, and the Department's laptops and workstations. Dell also provides help desk services and all personal computer services.

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. The 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. The 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.

In addition, the Department, through Federal Student Aid (FSA), administers programs that are designed to provide financial assistance to students enrolled in postsecondary education institutions, as well as to collect outstanding student loans. FSA has consolidated many of its student financial aid program systems into a general support system called the Virtual Data Center (VDC) to improve interoperability and reduce costs. The VDC 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 networks, mainframe computers, operating system platforms, and the corresponding operating systems. The VDC is also managed by Dell and is located at the contractor's facility in Plano, Texas.

[3] Formerly Perot Systems, which was acquired by Dell in September 2009.

AUDIT RESULTS

Based on the requirements specified in FISMA and the annual reporting instructions, our audit focused on 11 reporting metric areas of the Department's information security program — Continuous Monitoring, Configuration Management, Identity and Access Management, Incident Response and Reporting, Risk Management, Security Training, POA&M, Remote Access Management, Contingency Planning, Contractor Systems, and Security Capital Planning.

We determined that the Department's and FSA's IT security program generally complied with the E-Government Act of 2002 (Public Law 107-347), including Title III—Information Security, and related information security standards identified within Office of Management and Budget guidelines. However, we found that, while the Department has made progress in strengthening its information security program, many longstanding weaknesses remain and the Department's information systems continue to be vulnerable to serious security threats. Specifically, we determined that the Department was compliant with the Continuous Monitoring, Security Training, POA&M, Contractor Systems, and Security Capital Planning reporting metrics.[4] However, we identified findings in 6 of the 11 FY 2014 FISMA reporting metrics. In addition, we identified a finding regarding the implementation of corrective actions to address some of our previous recommendations.

Five of the six metric areas where we had findings contained repeat or modified repeat findings from the following OIG reports issued from FYs 2011 through 2013:

- "Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE)," September 2011 (ED-OIG/A11L0001);
- "The U.S. Department of Education's Compliance with the Federal Information Security Management Act for Fiscal Year 2011," October 2011 (ED-OIG/A11L0003);
- "Education Central Automated Processing System (EDCAPS) Information Security Audit," September 2012 (ED-OIG/A11M0002);
- "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).

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 on the draft report is included as Enclosure 2 to this report.

[4] Because the Department has consistently complied in recent years with POA&M, Contractor Systems, and Security Capital Planning requirements, we did not perform additional fieldwork for these security areas. Instead, we relied on work conducted during the FY 2013 FISMA audit.

FINDING NO. 1 – Configuration Management

The Department did not fully comply with this reporting metric.

Issue 1a. Configuration Management Policies, Procedures, and Plans Did Not Comply with NIST and Departmental Guidance

Although the Department established configuration management policies and procedures, it did not comply with current NIST and Departmental guidance. NIST Special Publication (SP) 800-53, Revision 3, "Recommended Security and Privacy Controls for Federal Information Systems and Organizations," "CM-1 Configuration Management Policy and Procedures," 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. OCIO defines this frequency as annually. Contrary to requirements, the Department's OCIO-11, "Handbook for Information Technology Security Configuration Management Planning Procedures," had not been updated since 2005, and the "Information Technology Security Baseline Configuration Guidance" had not been updated since 2009. Lack of current policies and procedures could result in a lack of sufficient information to determine the risk, threat frequency, and the ability to safeguard the Department's information.

Furthermore, the Department's configuration management plans were neither updated nor approved as required.[5] The Department's OCIO-11, "Handbook for Information Technology Security Configuration Management Planning Procedures," requires configuration management plans to be reviewed and updated "as needed—at least annually" —throughout the entire [system development life cycle]." In addition, OCIO-11 states that each system must have a configuration management plan that incorporates current configuration management standards. We found that 8 of the 16 (50 percent) sampled systems' configuration management plans were not updated in accordance with established Departmental timelines, with 1 dating back to 2009, 5 dating back to 2010, and 2 dating back to 2011-2012. We also found that the configuration management plans were neither approved nor finalized as directed by Departmental guidance. Without complete and up-to-date system configuration management plans, the Department may not be able to track configuration changes to systems.

FY 2014 Vulnerability and Penetration Testing Results

As part of our FY 2014 FISMA audit work, we conducted penetration and vulnerability testing of a major FSA system. While the testing team discovered that some systems were missing patches that resulted in high severity findings, we found that the number of findings identified was low.[6] Compared with organizations of similar size, the testing team determined that the

[5] NIST SP 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," CM-2 Baseline Configuration and OCIO-11, "Handbook for IT Security Configuration Management Planning Procedures."

[6] High severity refers to a rating determined from the Common Vulnerability Scoring System. This system, under the custodianship of NIST, is a free and open industry standard used for assessing the severity of computer system vulnerabilities by establishing a measure of how much concern a vulnerability warrants, compared to other vulnerabilities, so efforts can be prioritized.

contractor was performing a satisfactory job in ensuring that the patches and security configurations of the servers were met.

Recommendation

We recommend that the Deputy Secretary require OCIO to:

1.1 Update current configuration management policies, procedures, and plans in accordance with NIST and Departmental guidelines.

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.

FINDING NO. 2 – Identity and Access Management (Modified Repeat Finding)

The Department did not fully comply with this reporting metric.

Issue 2a. Identity Access and Management Process Needs Improvement (Modified Repeat Finding)

OCIO has still not fully established and implemented processes for identity and access management. Specifically, we found that the OCIO had not fully established policies and procedures to identify all devices that were attached to the network, distinguish those devices from users, and authenticate devices that were connected to the network. NIST SP 800-53, Revision 3, IA-2, "Identification and Authentication (Organizational Users)," and IA-3, "Device Identification and Authentication," require that information systems uniquely identify and authenticate users and specific devices before establishing a connection.

Although OCIO has taken several actions, it is still in the process of finalizing its implementation of an enterprise-wide Network Access Control (NAC) solution and implementing procedures for identity and access management in response to the OIG's recommendation from the FY 2011 FISMA report.[7]

Without the ability to account for and authenticate all devices connected to the network, the Department cannot effectively monitor, track, and authenticate all devices and users of the devices. Also, without proper logical access control in place, the Department cannot ensure that the identification and authentication controls are operating as intended and are preventing

[7] A NAC solution is a method of bolstering the security of a network by restricting the availability of network resources to endpoint devices that comply with a defined security policy.

unauthorized transactions or functions. Further, there is increased risk that unauthorized activities or excessive use of system resources could reduce the reliability and integrity of Department systems and its data, as well as the potential that sensitive data may be released, used, or modified. We also identified this condition in our FY 2011, 2012 and 2013 FISMA audits.

Issue 2b. Password Authentication Process Needs Improvement (Modified Repeat Finding)

The Department did not consistently follow and enforce the required Federal and Departmental guidelines requiring users to update their network passwords. OCIO-01, "Handbook for Information Assurance Security Policy," October 2011, states that passwords must be (1) obscured during login and during transmission, (2) changed after the initial login, and (3) forced by the system to be changed every 90 days.

To validate whether the Department was following and enforcing the 90-day password change requirement for all users, including both Federal employees and contractors, we requested a listing of all users and the date of all users' last password change as of July 21, 2014. We found that of the 6,597 users, 1,840 (28 percent) did not change their passwords for more than 90 days. We also found that the Department did not enforce the password change requirement by locking out users who did not change their passwords.

NIST SP 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," IA-5 Authenticator Management, requires agencies to manage information system authenticators for users and devices by establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators.

Password expiration policies exist to mitigate the issues that would occur if an attacker were to acquire the password hashes of a system and took action to exploit them. If an attacker were to acquire a user's shadow password file, they could then start brute forcing the passwords without further accessing the system.[8] Password policies help to decrease the potential for unauthorized users to obtain and use an account password.

Issue 2c. Users' Logical Access Controls Not Fully Implemented

FSA did not fully establish effective access controls for a major FSA system to ensure users of an application were not able to manipulate their user settings. Specifically, during penetration testing of this FSA system, the OIG's testing team was able to perform unauthorized actions by elevating the privileges of a basic user account. For example, the team modified the hypertext transfer protocol request and then gained access to portions of the system which we were not authorized to access.[9]

[8] A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number.

[9] Hypertext transfer protocol is the underlying protocol (set of rules) used by the World Wide Web. It defines what actions Web servers and browsers should take in response to various commands. When you enter a uniform resource locator into a browser, this actually sends a hypertext transfer protocol command to the Web server directing it to fetch and transmit the requested Web page.

NIST SP 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," AC-3 Access Enforcement, requires agencies to enforce approved authorizations for logical access to the system in accordance with applicable policy.

Without effective access controls in place, FSA runs the risk of allowing users to manipulate their access privileges and perform unauthorized actions that could compromise the confidentiality, integrity, and availability of the network and data.

Recommendations

We recommend that the Deputy Secretary require OCIO to:

2.1 Update and implement policies and procedures, including a NAC solution, consistent with NIST and FISMA guidelines to (1) identify all devices that are attached to the network; (2) distinguish the devices from users; and (3) authenticate devices that are connected to the network. (Modified Repeat Recommendation)

2.2 Develop and implement a detailed action plan on how OCIO-01, "Handbook for Information Assurance Security Policy" will be enforced to require that passwords are changed every 90 days. (Modified Repeat Recommendation)

We recommend that the Under Secretary require FSA to:

2.3 Restrict access rights so users of the major FSA system tested are allowed to access only authorized areas based on their pre-established roles.

We initially made the recommendation concerning the identity and access management process in FY 2011. In its corrective action plan for FY 2011, OCIO contracted for an engineering study that concluded that the implementation of a NAC solution on the network would allow the Department to (1) identify all devices that are attached to the network; (2) distinguish the devices from users; and, (3) authenticate devices that are connected to the network consistent with FISMA, OMB, and NIST guidance. While the Department completed its corrective actions in FY 2013, we noted that OCIO has consistently extended the implementation of the NAC solution and is still in the process of finalizing its implementation. Since we found the same conditions existed this year, we are making a modified repeat recommendation that emphasizes the need to implement a NAC solution.

We initially made the recommendation concerning password authentication in FY 2013. In its corrective action plan for our FY 2013 recommendation concerning passwords, OCIO stated it set the "Maximum Password Age" configuration on the network to 90 days. The Department stated that it had completed its corrections in FY 2013. However, during our fieldwork we found that more than a quarter of Departmental users did not change their passwords for more than 90 days. Consequently, we are making a modified repeat recommendation to develop a detailed action plan on how OCIO will address this issue.

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.

FINDING NO. 3 – Incident Response and Reporting (Modified Repeat Finding)

The Department did not fully comply with this reporting metric.

Issue 3a. Incident Response and Reporting to the United States Computer Emergency Readiness Team Needs Improvement (Modified Repeat Finding)

OCIO did not report security incidents to the United States Computer Emergency Readiness Team (US-CERT) consistent with NIST SP 800-61, Revision 2, "Computer Security Incident Handling Guide" and the "US-CERT Federal Incident Reporting Guidelines." OCIO officials stated the Department relies on the US-CERT standards category listings and timelines for incident response reporting. As outlined in the "US-CERT Federal Incident Reporting Guidelines," all computer incidents should be reported as follows: Category 1—unauthorized access—should be reported within 1 hour; Category 2—denial of service—should be reported within 2 hours if the successful attack is ongoing and the agency is unable to mitigate; Category 3—malicious code—should be reported daily, or within 1 hour if it is widespread across the agency; Category 4, improper usage (violation of security policy), should be reported weekly; and Category 5—scans, probes, or attempted access—should be reported monthly.

To determine whether OCIO complied with reporting security incidents to US-CERT, we judgmentally sampled 45 incident tickets from the Operational Vulnerability Management Solution (OVMS).[10] We found that 4 (9 percent) of the 45 sampled incidents were not reported to US-CERT as required. Specifically, we found that:

- For the four Category 1 and 2 incidents we reviewed, we found no reporting problems;
- One of the eleven Category 3 incidents from the OVMS was never reported to US-CERT after discovery/detection;
- Two of the twenty-six Category 4 incidents from the OVMS were never reported to US-CERT after discovery/detection; and
- One of the four Category 5 incidents from the OVMS was never reported to US-CERT after discovery/detection.

In accordance with NIST SP 800-61, Revision 2, all Federal agencies must ensure that their incident response procedures adhere to US-CERT's reporting requirements and that the

[10] The Department uses OVMS for the purpose of managing, coordinating and tracking the remediation of security weaknesses and vulnerabilities identified on behalf of its applications, information systems, and networks.

procedures are followed properly. Not reporting incidents to US-CERT as required could impede US-CERT's ability to properly analyze the information to identify trends and precursors of attacks. It is critical to notify US-CERT so it can effectively assist in coordinating communications with the other agencies in handling incident response and reporting. We also identified this condition in our FY 2011 and 2013 FISMA audits.

Issue 3b. Incident Response and Reporting to Law Enforcement Needs Improvement (Modified Repeat Finding)

The Department did not report security incidents to law enforcement in accordance with organizational procedures. To determine whether the Department correctly and timely reported incidents to law enforcement, we judgmentally sampled 45 incident tickets from OVMS. Based on our sample of the 45 incident tickets, a total of 17 incidents met the requirements to be reported to law enforcement. Of those 17 incidents, 16 (94 percent) were either not reported in a timely manner or not reported at all.

According to NIST SP 800-61, Revision 2, law enforcement should be contacted through designated individuals in a manner consistent with the requirements of the law and the organization's procedures. In addition, OCIO-14 "Handbook for Information Security Incident Response and Reporting Procedures," states that incidents that may constitute a computer crime (violations of applicable Federal or State laws) must be reported to the OIG Technology Crimes Division. These incidents may include, but are not limited to, the following:

- compromise of system privileges (root access),
- compromise of information protected by law,
- events that include exposure or release of Personally Identifiable Information,
- unauthorized access of the Department's IT systems and/or electronic data,
- exceeding authorized access of the Department's IT systems and/or electronic data,
- denial of service of major IT resources,
- child pornography, and
- malicious destruction or modification of the Department's data or information (Website defacement).

The failure to provide law enforcement timely incident reports may directly impede criminal investigative activities and jeopardize the success of detection. If incidents are not reported as soon as possible, information that is vital to the securing of evidence may be lost, and law enforcement agencies may lose the ability to make important connections to ongoing cases and decisions about initiating new cases. We also identified this condition in our FY 2013 FISMA audit.

Recommendations

We recommend that the Deputy Secretary require OCIO to:

3.1 Develop and implement a detailed action plan of how existing policies and procedures will be fully implemented to ensure security incidents are reported to US-CERT within the required timeframes. (Modified Repeat Recommendation)

3.2 Develop and implement a detailed action plan of how existing policies and procedures will be fully implemented to ensure applicable security incidents are correctly and timely reported to law enforcement. (Modified Repeat Recommendation)

A recommendation similar to 3.1 was made in FY 2013 and corrective action was completed in FY 2014. In its corrective action plan, OCIO stated that it developed a new policy called the "Cyber Security Operations Standard Operating Procedure OIG Incident Coordination," dated January 14, 2014, to reflect reporting criteria and provide a user communication plan to ensure that third party customers are aware of and respond to US-CERT reportable incidents in a timely manner. The Department stated that it had completed this corrective action in FY 2014, but during our fieldwork we continued to find that incidents were still not reported to US-CERT as required. Consequently, we are making a modified repeat recommendation to develop a detailed action plan on how OCIO will address this issue.

A recommendation similar to 3.2 was made in FY 2013 and corrective action was completed in FY 2014. In its corrective action plan, OCIO again stated that it developed the "Cyber Security Operations Standard Operating Procedure OIG Incident Coordination," dated January 14, 2014, to reflect reporting criteria to include the required documentation for the notifications. The Department stated that it had completed this corrective action in FY 2014, but during our fieldwork we continued to find that incidents were still not reported to OIG as required. Consequently, we are making a modified repeat recommendation to develop a detailed action plan on how OCIO will address this issue.

Management Comments

The Department partially concurred with the recommendations. For Recommendation 3.1, the Department stated that currently OVMS does not allow the downgrading of events after an entry is initially created and that if an event is created as a category (CAT #), it retains that CAT # designation in the system until resolved. As a result, several of the identified events were deemed not reportable, downgraded before reporting, or downgraded by US-CERT. OCIO, in conjunction with FSA, has conducted market research and is acquiring a new tool specifically focused on incident handling that will address this limitation. The new solution is currently scheduled to be in production by June 30, 2015. In addition, the Cybersecurity Operations US-CERT reporting guide will be modified to add a daily audit by the Education Security Operations Center Management Team and a weekly audit by a government team member to ensure appropriate and timely reporting. The target completion date is December 30, 2014.

For Recommendation 3.2, the Department stated that the previous year's corrective action plan was implemented in January 2014, with a revision in March 2014, and the majority of the cited events occurred before the corrective action plan was completed. In addition, OCIO will meet with OIG's Technology Crimes Division to validate the incidents that require notification. Any changes to OCIO-level existing processes will be updated by December 30, 2014. For documents that require Department-wide review and coordination, the process will be started by January 30, 2015.

OIG Response

For Recommendation 3.1, the Department did not provide any further evidence to support that some of the incidents cited were later deemed not reportable and downgraded before reporting or downgraded by US-CERT. In addition, we were not informed of this limitation in OVMS during our testing of these incidents. Further, if OVMS prevented changes to the initial designation assigned to an incident, we would have expected to see documentation explaining this limitation.

For Recommendation 3.2, although the Department stated that a majority of the cited incidents occurred before the corrective action plan was completed (January 2014), we still found that 5 incidents occurring after January 2014 were either not reported in a timely manner or not reported at all. A complete validation of this corrective action will be conducted during our FY 2015 FISMA work.

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

FINDING NO. 4 – Risk Management (Modified Repeat Finding)

The Department did not fully comply with this reporting metric.

Issue 4a. Risk Management Program Is Not Fully Implemented (Repeat Finding)

The Department has still not fully implemented NIST SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems," February 2010. Since 2010, the OCIO has been in the process of updating and implementing the risk management policies and procedures for continuous security authorization to be in accordance with NIST 800-37, Revision 1. During the past four years, OCIO has extended the completion date several times from its original October 2012 planned completion date. As a result, personnel do not have Departmental guidance that is consistent with NIST guidance on the risk management framework, and the Department may be authorizing systems to operate on the network that are not in accordance with the most current NIST guidelines. We also identified this condition in our FY 2011, 2012 and 2013 FISMA audits.

Issue 4b. System Authorization Process Needs Improvement (Modified Repeat Finding)

The Department's system authorization process needs improvement. Our review identified many deficiencies in system security plans, authorization to operate documents, security assessment reports, and expired system authorizations (formerly called certification and accreditation).

As of March 2014, the Department reported a total of 242 systems in its inventory. Of the 242 systems, we found that 72 systems (30 percent) have been operating on the Department's network on expired system authorization documentation to include security authorizations, self-assessments dates, and contingency plans that were not timely tested. Specifically, from the reported 242 systems we identified:

- 58 (24 percent) were operating on expired security authorizations,
- 41 (17 percent) were operating on expired self-assessment dates, and
- 49 (20 percent) were operating on expired contingency plans that were not timely tested.

Further, for a more in-depth review of the system authorization process for the Department's risk management program, we judgmentally selected 16 of the 242 systems. Of the 16 systems we reviewed, we found that:

- two systems did not have a consistent Federal Information Processing Standards Publication 199 system categorization level for its system security plan; [11]
- five systems did not contain proper support for the system interconnections; and
- two systems had authority to operate letters that were over three years old.

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. Providing orderly, disciplined, and timely updates to the security plan, security assessment report, and POA&M 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 authorization to operate, the Department did not have adequate controls in place to ensure the effective and consistent certifying and accrediting of systems within the required 3-year timeframe, which allowed security authorizations to expire. As a result, Department operations and assets can be exposed to significant security risks until such security weaknesses are corrected or mitigated. We also identified this condition in our FY 2011, 2012 and 2013 FISMA audits.

Recommendations

We recommend that the Deputy Secretary require OCIO to:

4.1 Develop and implement a detailed action plan to ensure that all system authorization documentation is readily available and complies with Federal and Department standards and guidance, and take immediate action to resolve the deficiencies identified (a list of systems and applicable documentation was provided to OCIO). (Modified Repeat Recommendation)

4.2 Develop and implement controls to ensure timely re-authorizations for systems, avoiding gaps in authority to operate coverage. (Modified Repeat Recommendation)

[11] Federal Information Processing Standards Publication 199 system categorization levels are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

A recommendation similar to 4.1 was made in FY 2011 and corrective action was completed in FY 2012. In the completion of its corrective action plan for this finding, OCIO stated that OCIO-05 "Handbook for Information Technology Security Certification and Accreditation Procedures," dated March 6, 2006, would be revised to require that all system authorization documentation be uploaded to OVMS to ensure it is readily available. However, to date, OCIO-05 has not been revised. Since we found the same conditions existed this year, we are issuing modified repeat recommendation that focuses on the need to develop and implement a detailed action plan.

A recommendation similar to 4.2 was made in FY 2011 and corrective action was completed in FY 2012. In its corrective action plan, the Department stated that it would implement procedures to ensure OVMS automated tracking was being utilized to track Department systems reaccreditation and recertification and that this procedure will be finalized by October 30, 2012. However, we continued to find that the Department is not timely completing the reauthorizations. Therefore, we are making a modified repeat recommendation that focuses on the need to develop and implement a detailed action plan.

In addition, for Issue 4a, we are not making an additional recommendation. We initially made the recommendation concerning this condition in FY 2011. Although OCIO is working on implementing a risk management program, corrective actions are still not completed because the implementation process is taking longer than originally planned.

Management Comments

The Department partially concurred with the recommendations. For Recommendation 4.1, the Department stated it has made significant efforts towards improving system security documentation and ensuring that it is readily available and complies with Federal and Department standards and guidance. OCIO has worked extensively with program offices, authorizing officials, system owners, and information system security officers through monthly meetings, targeted workshops, and one-on-one sessions in order to communicate requirements, provide templates and resources, and provide any guidance necessary. Through OCIO's concerted efforts and collaboration with program offices to properly dispose of systems, accurately characterize and document systems, and increase understanding of overall information system security requirements, the Department has experienced improvements. For the list of systems cited in the report, OCIO will ensure all documentation gaps are addressed by March 31, 2015.

For Recommendation 4.2, the Department stated it has made significant efforts towards improving the system authorization process, and since the OIG's fieldwork was completed, the Department's system inventory has been reduced to 164 FISMA reportable systems. Of the 164 systems, 31 (19 percent) are currently operating with invalid authorities to operate, but 16 of the systems have been through the assessment process and are currently pending final authority to operate signatures. OCIO is progressing with its implementation of an enterprise-wide risk management framework in accordance with NIST 800-37, and will publish guidance to address the initial and ongoing authorization of systems by June 30, 2015.

OIG Response

Although the Department stated it has made significant efforts towards improving system security documentation and the system authorization process, we continue to find many deficiencies in system security plans, authorization to operate documents, security assessment reports, and expired system authorizations. In addition, for Recommendation 4.2, the Department did not provide any further evidence to support that its system inventory has been reduced and that only 31 systems are currently operating with invalid authorities to operate. However, the Department's planned corrective actions, if properly implemented, are responsive to the finding and recommendations.

FINDING NO. 5 – Remote Access Management (Modified Repeat Finding)

The Department did not fully comply with this reporting metric.

Issue 5a. Lack of Inventory over Universal Serial Bus Storage Drives

OCIO did not have effective internal controls over its inventory of Universal Serial Bus (USB) storage drives. Although each Departmental office is allowed to purchase, inventory, and manage its own USB devices, OCIO did not have a centralized inventory of these drives. In addition, when individual Department offices purchased new encrypted USB drives that met the Department's standards, previously issued unencrypted drives were never recovered. Further, we identified an instance in which the Department reported that during FY 2014, a user lost a Department issued unencrypted USB drive that contained Departmental data. According to OMB Circular A-130, the Department is required to keep a complete inventory of agency information resources, including equipment devoted to information resources management and information technology. When requested by OIG, OCIO was not able to produce an inventory of all distributed USB drives to employees or contractors. OCIO also stated that there was no effort made to retrieve and destroy the previously issued unencrypted USB drives, and that it was left up to each individual Department office to replace them. Failure to properly account for its USB drives could lead to data leakage or exposure of sensitive Departmental information, especially for unencrypted USB drives.

Issue 5b. The Department is [redacted]

The Department [redacted] The failure to restrict unauthorized devices from connecting to the Department's network led to the introduction of a virus via a contractor that connected an unapproved system to an unrestricted port. According to NIST SP 800-46, Revision 1, "Guide to Enterprise Telework and Remote Access Security," organizations should use a NAC solution whenever feasible to detect major security policy violations in telework client devices and to prevent teleworkers from inadvertently using the wrong device for telework. [redacted] Failure to detect unauthorized devices leads to spoofing and the introduction of unauthorized devices into the network. [redacted]

(b)(7)(E)

Issue 5c. FSA Continues Use of Social Security Numbers as a Primary Identifier

FSA did not have an adequate solution to phase out the use of social security numbers (SSN) or other PII as the primary identifier when accessing user account information via the Internet. In accordance with OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," agencies were required to establish a plan to eliminate the unnecessary collection and use of SSNs as a personal identifier for both Federal employees and in Federal programs (e.g., surveys and data calls). Our review of the nslds.ed.gov and the fafsa.ed.gov web sites (both publicly accessible) revealed that users are asked to provide SSNs to authenticate. FSA explained that the use of SSNs for account management was necessary and required for a valid agency purpose. However, our primary concern is that the continued use of SSNs as the primary identifier when authenticating via a public web site could increase the risk of PII exposure and ultimately identity theft.

Issue 5d. Lack of Restrictions for Virtual Private Network Client Programs on non-Government Furnished Equipment

OCIO does not restrict users from connecting to the Department's network via a virtual private network client program with the use of non-Government Furnished Equipment (GFE).[12] OIG was able to validate this condition by downloading the same type of Department approved virtual private network client from an open source Internet site and installing it on a non-GFE computer. Once installed and configured with the proper settings, the client allowed OIG to connect to the internal Department network. According to NIST SP 800-46, Revision 1, organizations should use a NAC solution whenever feasible to detect major security policy violations in telework client devices and to prevent teleworkers from inadvertently using the wrong device for telework. In addition, NIST SP 800-46, Revision 1, states that organizations should assume that client devices will become infected and plan their security controls accordingly. OCIO has not implemented a NAC solution, or another alternate solution, that would allow validation of the security posture of non-GFE devices connecting to the Department's network. During FYs 2013 and 2014, vendors introduced multiple viruses and malware to the Department's network, thus putting the network at risk for data exposure and the introduction of security vulnerabilities and malware. A system that has not had its security posture validated could be used to upload/download information without any restrictions.

Issue 5e. Mobile Devices with Root Access Are Allowed to Connect to the Network

OCIO cannot validate if Windows mobile devices have been rooted before allowing them to connect to the Department network. Rooting is the process by which one gains access to the administrative commands and functions of a mobile device's operating system, therefore granting the user unlimited privileged control of the device. According to NIST SP 800-124, Revision 1, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," the use

[12] A virtual private network connects two systems securely and privately over the Internet. A virtual private network client on one system connects to a virtual private network server on another system and by using encryption; only the two parties connected can see what information is being exchanged.

of rooted mobile devices should be automatically detected when feasible. OCIO confirmed that it currently has no technical ability to validate if certain mobile devices connected to the network have been rooted, specifically the mobile devices not configured under the McAfee Enterprise Mobility Management platform. OCIO provided a risk acceptance form to address certain vulnerabilities discovered with its mobile device management solutions; however, the risk acceptance form does not the address the vulnerability of allowing rooted mobile devices to connect to the Department network. Failure to validate if a mobile device has been rooted could lead to exposure of credentials and other sensitive data since the device would have unlimited privilege controls.

Issue 5f. Data Storage on Mobile and External Storage Devices Process Needs Improvement (Modified Repeat Finding)

OCIO does not use encryption on mobile devices and external storage devices to protect Departmental data. The Department's current mobile device management solution does not allow mobile devices to be encrypted with full-disk encryption, nor does it have the capability to enforce encryption of external storage devices.[13] OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," states that agencies should encrypt, using only NIST-certified cryptographic modules, all data on mobile computers and devices carrying agency data unless the data are determined to be not sensitive. In addition, NIST SP 800-111, "Guide to Storage Encryption Technologies for End User Devices," states that an organization's devices (including desktop computers) may be configured to prevent writing sensitive information to removable media, such as compact disks or USB storage devices, unless the information is properly encrypted. Unencrypted information stored on mobile devices and external storage devices could be leaked if the device is stolen, as there is no protection from the data at rest. Using whole disk encryption on mobile devices would provide an additional layer of security. We also identified this condition in our FY 2013 FISMA audit.

Issue 5g. Two-Factor Authentication Not Fully Implemented (Modified Repeat Finding)

OCIO still has not fully implemented and enforced the use of two-factor authentication when accessing the Department's systems to comply with Department of Homeland Security and OMB guidance requiring two-factor authentication.[14] For instance, OIG was able to validate that two-factor authentication was not implemented for accessing webmail and the G5 application.[15] OCIO informed OIG that it intends to retire the single-based authentication for webmail by September 2014; however, as of October 2014 the webmail single-based authentication access has yet to be retired. In addition, [redacted] This allowed users to access PII via this application without having to dual-authenticate or even authenticate at all

[13] Full-disk encryption is a type of encryption at the hardware level that converts data on a hard drive into a form that cannot be understood by anyone who does not have the key to undo the conversion.
[14] Homeland Security Presidential Directive (HSPD)-12, "Policy for a Common Identification Standard for Federal Employees and Contractors;" OMB memorandum M-06-16, "Protection of Sensitive Agency Information;" and OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information."
[15] The G5 application is the Department's grants management system and is available to applicants, grantees, payees as well as internal staff.

(based on the programming issue). Although OCIO has enabled personal identity verification authentication for internal users on the G5 application, external users can authenticate via single sign-on. Allowing users to sign on without two-factor authentication could expose data, 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 system and the data at risk for exposure from unauthorized users. We also identified this condition in our FY 2011, 2012 and 2013 FISMA audits.

Issue 5h. Data Transmission and Storage Restriction Can Be Bypassed (Repeat Finding)

By allowing users to use cloud storage and file sharing services (such as Google Drive), the Department continues to allow employees to bypass restrictions for transmitting data and storing agency information on unencrypted public cloud solutions. OCIO-01, "Handbook for Information Assurance Security Policy," requires users to use e-mail systems when electronically sending and receiving government information, as well as encrypting all sensitive but unclassified data. OMB Memorandum M-06-16, "Protection of Sensitive Agency Information," states that when PII is being stored at a remote site, NIST SP 800-53 should be implemented to ensure the information is stored only in encrypted form. However, OCIO-01 does not contain any guidance about the transmission and storage of data using public cloud solutions. We also noted that the terms of service for one public cloud provider allowed the provider to use, store, reproduce, create and publicly display and distribute the content uploaded to its services. By allowing users to circumvent network restrictions to transmit and store data, the Department increases the risk of data exposure to unauthorized sources. This is especially important since the Department collects and maintains a significant amount of PII about employees, students, and other Department customers. We also identified this condition in our FY 2013 FISMA audit.

Issue 5i. Policy on Removable Storage Devices Needs Improvement (Repeat Finding)

The Department still does not have a process in place to scan removable storage devices to validate their security posture when connected to GFE computers. NIST SP 800-53, Revision 3, states that portable, removable storage devices (such as thumb drives, flash drives, and external storage devices) can be the source of malicious code insertions into organizational information systems and recommends scanning the devices. Departmental guidance does not currently require that removable storage devices be scanned when connected to a GFE computer. Since the Department allows the use of Department-issued removable storage devices on non-GFE, not scanning those removable devices for security concerns such as malware and viruses creates the possibility that malicious anomalies could be introduced to the network from the non-GFE. We also identified this condition in our FY 2013 FISMA audit.

Recommendations

We recommend that the Deputy Secretary require OCIO to:

5.1 Update its asset management policy to ensure that USB drives are recorded and maintained in a centralized asset management solution, and properly disposed of upon their end-of-life.

5.2 Enable a NAC, (b)(7)(E) capable of detecting and protecting the network against unauthorized connections.

5.3 Restrict unauthorized systems from connecting to the network via a virtual private network client solution.

5.4 Restrict rooted mobile devices from connecting to the network and continuously monitor authorized mobile devices to validate if they have been rooted.

5.5 Enable full disk encryption on mobile devices and external storage devices that store sensitive Departmental data.

5.6 Enable dual-authentication via all external connections to the G5 application.

We recommend that the Under Secretary require FSA to:

5.7 Eliminate the use of SSNs as the primary identifier when authenticating onto FSA web sites by requiring the user to create a unique identifier for account authentication.

For the repeat findings, we are not making any additional recommendations. Corrective actions to address five recommendations contained in the FY 2011, 2012 and 2013 FISMA reports are still not completed.

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.

FINDING NO. 6 – Contingency Planning (Modified Repeat Finding)

The Department did not fully comply with this reporting metric.

Issue 6a. Information System Contingency Plans Not Complete (Modified Repeat Finding)

OCIO did not consistently document the IT recovery procedures for its systems in accordance with NIST guidelines and Departmental policies. Specifically, we found that of the 16 system contingency plans, 6 (38 percent) did not include all the required information system contingency planning elements identified in NIST guidelines and Departmental guidance.[16]

[16] 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."

Specifically, we found that these six information system contingency plans collectively did not (1) identify the roles and responsibilities of key individuals and functions; (2) document key individuals' contact information in the event of a disaster; (3) document training requirements; (4) identify an alternate storage site for system backups; (5) provide a description of backup procedures to include the frequency of backups and offsite storage instructions; (6) identify an alternate processing site when required; (7) document planned testing, exercise and maintenance activities; or (8) identify the alternate telecommunication services when required. This occurred because OCIO did not ensure contingency plans included all required elements in accordance with NIST guidelines for developing effective plans.

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. Proper contingency planning is necessary to ensure that services provided by systems are able to operate effectively without excessive interruption. Without proper contingency planning, systems may not be able to recover quickly following a service disruption or disaster. We also identified this condition in our FY 2011, 2012 and 2013 FISMA audits.

Issue 6b. Information System Contingency Plan Testing Process Needs Improvement (Modified Repeat Finding)

OCIO and FSA did not consistently perform and document contingency plan testing in accordance with NIST guidelines and Departmental guidance. For 9 of the 16 (56 percent) systems, we were provided evidence indicating that contingency plan testing was not performed on an annual basis as required. OCIO and FSA officials did not consistently require Information System Security Officers or system owners to perform and document contingency plan tests for all the Department systems in accordance with NIST guidelines and Departmental procedures.

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-01, "Handbook for Information Assurance Security Policy," requires all contingency plans for systems to be tested annually and the results of the tests documented and used to update the contingency plan and POA&M items created as a result, if necessary. If the Department does not perform and document contingency plan tests, it is unable to validate recovery capabilities and identify or correct the deficiencies in the contingency plans. We also identified this condition in our FY 2012 FISMA audit.

Recommendations

We recommend that the Deputy Secretary require OCIO to:

6.1 Review and update information system contingency plans for the six systems that have elements missing to ensure that all the contingency planning elements are included as required by NIST guidelines and Departmental guidance.

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

6.2 Perform and document contingency plan test results for the nine systems in question as required by NIST guidelines and Departmental procedures.

6.3 Develop and implement a detailed action plan to ensure Information System Security Officers and/or system owners are performing and documenting annual contingency plan testing for all Departmental systems as required by NIST guidelines and departmental procedures. (Modified Repeat Recommendation)

A recommendation similar to 6.3 was made in FY 2012 and corrective action was completed in FY 2013. In the completion of its corrective action plan for FY 2012, OCIO stated that it would leverage reporting from OVMS and monthly meetings to ensure Information System Security Officers and system owners were aware of the requirement to perform annual contingency plan testing. While we found that systems owners were made aware of the requirement, for the systems we sampled, these conditions continued to exist this year. Consequently, we are issuing a modified repeat recommendation focusing on ensuring that system owners are performing and documenting annual contingency plan testing.

In addition to the recommendations made above, corrective action to address the recommendation from our FY 2013 FISMA report to review all the Departmental systems contingency plans to ensure that all required information is included in each plan as required by NIST guidance is still not completed.

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.

FINDING NO. 7 – Implementation of Corrective Action Plans

The Department's process for implementing corrective actions needs improvement. Specifically, we found that the Department did not perform adequate remediation of weaknesses identified in previous OIG audit reports resulting in repeat and modified repeat conditions in this report. For FY 2014, we identified repeat and modified repeat findings in 5 of the 11 reporting metrics based on reports issued during FY 2011 through 2013. We found that although the Department determined it had completed corrective actions on findings identified within each report, we found that some corrective actions have not been completed and that findings persisted. For example, in closing out its corrective action plan in FY 2012 for recommendations addressing contingency planning, the Department stated that it would leverage reporting from OVMS and monthly meetings to ensure Information System Security Officers and system owners were aware of the requirement to perform annual contingency plan testing. However, for this year's

contingency planning reporting, we continued to find that many information system contingency plans were not being tested annually as required.

During this year's fieldwork, we reviewed five reports issued during FYs 2011 through 2013 to determine whether the Department had taken action on implementing the recommendations in the reports.[17] We found that although the Department had completed 109 of the 118 recommendations (92 percent), the corrective actions for 7 recommendations (approximately 6 percent) reported as completed, resulted in the same or similar conditions this year, as follows:

- 2 recommendations from Identity and Access Management from the FY 2011 and FY 2013 FISMA reports;
- 2 recommendations from Incident Response and Reporting from the FY 2013 FISMA report;
- 2 recommendations from Risk Management from the FY 2011 FISMA report; and
- 1 recommendation from Contingency Planning from the FY 2012 FISMA report.

We also identified instances where the Department did not implement corrective actions in a timely manner. We found that the Department revised its original planned completion dates for 43 of its 154 corrective actions (28 percent).[18] For 37 these 43 corrective actions, the Department did not provide justification for revising the original planned completion date as required. In addition, 15 of the 154 corrective actions (10 percent) were completed late without the Department revising the planned completion date.

OMB Circular A-50, "Audit Followup," dated September 1982, requires that agency heads are responsible for assuring that management officials throughout the agency understand the value of the audit process and are responsive to audit recommendations. In addition, the audit follow-up official has personal responsibility for ensuring that timely responses are made to all audit reports and corrective actions are actually taken. Furthermore, according to the Officer of the Chief Financial Officer Directive 1-106, "Audit Resolution and Follow-up," dated January 2013, the Chief Financial Officer delegates the responsibility to each Department Principal Office for developing corrective action plans for internal audit findings and recommendations issued to that Principal Office and conducting additional audit follow-up responsibilities for internal and external audits, including monitoring and implementing corrective actions and requesting audit closure.

Effective audit follow-up is an integral part of having sound internal controls and is a shared responsibility of agency management officials and auditors. Timely and effective corrective action taken by management on findings and recommendations is essential to improving the effectiveness and efficiency of Government operations.

[17] ED-OIG/A11L0003; ED-OIG/A11L0001; ED-OIG/A11M0002; ED-OIG/A11M0003; and ED-OIG/A11N0001.
[18] For some findings, multiple corrective actions were included within a single recommendation.

Recommendations

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

7.1 A verification of completed corrective actions is performed prior to entry into the Department's Audit Accountability and Resolution Tracking System to ensure that recommendations are correctly addressed.

7.2 Completion dates for corrective action plans are revised appropriately and that justification is provided to support revised completion dates.

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.

OTHER MATTERS

During the course of the audit, we analyzed information, performed testing, and observed testing that relates to the Department's information security program and practices. Although this work was not included in the metric reporting section, the results of this work were significant enough to include it in this year's FISMA reporting.

EDUCATE Disaster Recovery Exercise

In June 2014, we observed the Department's execution of its disaster recovery exercise for the EDUCATE environment at its hot site facility in Florence, Kentucky.[19] We determined that the recovery exercise was executed in accordance with the documented plans and timelines. The following observations were made during our review of the exercise:

- Disaster recovery processes and procedures were tested and executed successfully.
- All EDUCATE applications designated for testing were successfully loaded.
- All issues identified were resolved during the exercise.
- The disaster recovery team demonstrated its ability to recover operations in the event of a disaster.
- During the exercise, the Client Access Servers restored at the hot site were not working properly. After directing Client Access Server functions back to the Plano Technology Center and rebooting the servers at the hot site, functionality at the hot site was restored and tested successfully.

Agency-wide Cloud Computing Initiative

During FY 2014, in a collaborative effort with the United States Department of Agriculture (USDA) OIG and other Federal OIGs, we participated in the Council of the Inspectors General on Integrity and Efficiency's agency-wide cloud computing initiative. The purpose of this project was to evaluate agencies' contracts for cloud services to determine whether the efforts to adopt cloud-computing technologies and transition to a cloud-computing model are in compliance with applicable standards and best practices. As part of the evaluation, each participating OIG was asked to perform a number of tasks, including evaluating a judgmentally selected sample of contracts between the Department and the cloud service providers.

We reviewed 3 of 10 commercial cloud service contracts, and found that the selected contracts were not compliant with the Federal Risk and Authorization Management Program (FedRAMP) and were not compliant with the recommended Federal Acquisition Regulation clause for allowing agency personnel access to cloud service provider facilities or with best practices recommended by the CIO Council and the Chief Acquisition Officers (CAO) Council related to investigative and audit access. Further, we found that none of the contracts contained a term of

[19] Hot sites are facilities appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel.

service agreement and service level agreements were not included in two of the contracts. In June 2014, we provided the results of our review to USDA OIG which then consolidated the results of the participating Federal agencies into a report that provided an overall view of Federal cloud computing environments.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of our audit was to determine whether the Department and FSA's overall IT security program and practices were in compliance with the E-Government Act of 2002 (Public Law 107-347) including Title III—Information Security, and related information security standards identified within OMB guidelines. We also assessed the implementation of corrective action plans by the OCIO and FSA.

This audit satisfies the FISMA requirement for us to perform an annual independent evaluation to determine the effectiveness of the Department's information security program and practices. As required by the FY 2014 FISMA Reporting Metrics, each Inspector General was required to evaluate its respective agency on the following 11 security areas: Continuous Monitoring Management; Configuration Management; Identity and Access Management; Incident Response and Reporting; Risk Management; Security Training; POA&M; Remote Access Management; Contingency Planning; Contractor Systems; and Security Capital Planning.[20]

To accomplish our objective, we performed the following procedures:

- reviewed applicable information security regulations, standards and guidance;
- gained an understanding of IT security controls in place 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 individuals with specific 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 2014 Inspector General FISMA reporting metrics;[21] and
- compared and tested management, operational, and technical controls in place based on NIST standards and Department guidance.

As of March 2014, the Department reported an inventory of 242 IT systems. We judgmentally selected 16 of the Department's IT systems to ascertain the security control aspects relating to Risk Management, Configuration Management, and Contingency Planning.[22] Of the 16 systems selected, we included 5 from the judgmental sample selected as part of our FY 2013 FISMA

[20] Because the Department has consistently complied with POA&M, Contractor Systems, and Security Capital Planning requirements, we did not perform fieldwork for these three security areas, and instead relied on work conducted during the FY 2013 FISMA audit.
[21] This procedure included OIG's reporting requirements for the OMB Memorandum M-14-03, "Enhancing the Security of Federal Information and Information Systems," which were included as part of the Continuous Monitoring reporting metric.
[22] Because we did not select a statistical random sample, any results found during our analysis were not projected across the entire inventory of Department IT systems.

audit. We selected these systems in order to measure progress from the prior fiscal year. We then selected 3 systems that were included as part of the FY 2014 EDUCATE Disaster Recovery Exercise. The remaining 8 systems were selected based on Departmental principal offices with a high, medium and low concentration levels of systems relative to the inventory of 242 Department systems. The table below lists the systems selected, the system's Principal Office, and the Federal Information Processing Standards Publication 199 potential impact level.

Number	System Name	Principal Office	Impact Level
1	Common Origination & Disbursement	FSA	MODERATE
2	Financial Management System	FSA	MODERATE
3	Central Processing System	FSA	MODERATE
4	Nelnet Commercial System	FSA	MODERATE
5	Rational Environment	FSA	MODERATE
6	ED.gov (Infrastructure)	OCIO	MODERATE
7	Education Central Automated Processing System	OCIO	MODERATE
8	EDUCATE Security	OCIO	MODERATE
9	Presidential Scholars Application Online	OCO*	MODERATE
10	Case and Activity Management System	OGC*	MODERATE
11	Education Investigative Tracking System	OIG	MODERATE
12	FOIA Tracking and Reporting System	OM*	MODERATE
13	Education Security Tracking and Reporting System	OM	HIGH
14	Teacher Quality Enhancement Title II Scholarship and Administration Reporting System	OPE*	MODERATE
15	Correspondence Control Manager	OS*	MODERATE
16	Rehabilitation Services Administration Management Information System	OSERS*	MODERATE

* Office of Communications and Outreach (OCO); Office of the General Counsel (OGC); Office of Management (OM); Office of Postsecondary Education (OPE); Office of the Secretary (OS); Office of Special Education & Rehabilitative Services (OSERS).

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 and Remote Access Management metric areas to support the findings summarized in this report. A limited assessment of the data was performed to assist in determining the reliability of the computer-processed data. We found the computer-processed data to be sufficiently reliable for the purposes of our review.

During FY 2014, in a collaborative effort with USDA OIG and other Federal OIGs, we participated in the agency-wide cloud computing initiative. The purpose of this project was to evaluate agencies' contracts for cloud services to determine whether the efforts to adopt cloud-computing technologies and transition to a cloud-computing model were in compliance with applicable standards. As part of the evaluation, each participating OIG was asked to perform a number of tasks, including:

- determining an enterprise-wide inventory of cloud IT services and service providers and selecting a judgmental sample of providers for evaluation;

- reviewing documentation for the selected contracts and service level agreements that have been executed between the agency and the cloud service provider to determine whether the contracts contain clearly defined roles, recommended Federal Acquisition Regulation clauses, and evidence of Federal Risk and Authorization Management Program compliance; and
- reviewing documentation for the selected contracts to determine whether the Department has a process in place to effectively manage its cloud computing providers to ensure it meets its contractual obligations.

We identified an inventory of 10 Departmental systems that utilized some form of commercial cloud services. For our sample, we judgmentally selected three systems to perform our evaluation of the Department's procurement process for cloud services. We performed our work based on a portion of USDA's established audit objective, scope, and methodology. For this cloud computing initiative, we did not perform all procedures as required by generally accepted government auditing standards, specifically for planning and overall evidence assessment. We obtained evidence that would support USDA's overall audit and provide reasonable assurance for our findings and conclusions. The work performed for this project did not affect our audit objective or the results of our audit.

To assess the Department's progress in implementing corrective actions to correct information security weaknesses identified in prior OIG audit reports, we reviewed 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 2013.[23] The information included planned, revised, and actual corrective action completion dates.

We conducted our fieldwork from January 2014 through July 2014, primarily at Departmental offices in Washington, D.C., and contractor facilities in Columbus, Georgia, and Florence, Kentucky. During our fieldwork, penetration and vulnerability testing was performed at a major FSA system's data center in Columbus, Georgia. We also performed an observation of a disaster recovery exercise at the EDUCATE recovery site in Florence, Kentucky during the month of June 2014. We held an exit conference on September 17, 2014.

Except for our work under the cloud computing initiative, included in the "Other Matters" section of this report, 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.

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

Enclosure 1: CyberScope FISMA Reporting Metrics

Inspector General

Section Report

2014

Annual FISMA Report

Department of Education

Section 1: Continuous Monitoring Management

1.1 Has the organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems 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: The U.S. Department of Education (Department) has established and is maintaining a continuous monitoring management program consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

1.1.1 Documented policies and procedures for continuous monitoring (NIST SP 800-53: CA-7).

Yes

Comments: No exceptions noted.

1.1.2 Documented strategy for information security continuous monitoring (ISCM).

Yes

Comments: No exceptions noted.

1.1.3 Implemented ISCM for information technology assets.

Yes

Comments: No exceptions noted.

1.1.4 Evaluate risk assessments used to develop their ISCM strategy.

Yes

Comments: No exceptions noted.

1.1.5 Conduct and report on ISCM results in accordance with their ISCM strategy.

Yes

Comments: No exceptions noted.

1.1.6 Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST SP 800-53, 800-53A).

Yes

Comments: No exceptions noted.

Section 1: Continuous Monitoring Management

1.1.7 Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as a common and consistent POA&M program that is updated with the frequency defined in the strategy and/or plans (NIST SP 800-53, 800-53A).

Yes

Comments: No exceptions noted.

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

Not used.

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?

Yes

Comments: The Department has established a security configuration program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines, but needs to make improvements to specific attributes as noted below.

2.1.1 Documented policies and procedures for configuration management.

No

Comments: "The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014," Audit Control Number ED-OIG/A11O0001, hereafter referred to as FISMA Report, Finding No. 1, Configuration Management, Issue 1b - Configuration Management Policies, Procedures, and Plans Did Not Comply with NIST and Departmental Guidance.

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.

Section 2: Configuration Management

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

Yes

Comments: No exceptions noted.

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

Yes

Comments: No exceptions noted.

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

Yes

Comments: No exceptions noted.

2.1.7 Process for timely and secure installation of software patches.

Yes

Comments: No exceptions noted.

2.1.8 Software assessing (scanning) capabilities are fully implemented (NIST SP 800-53: RA-5, SI-2).

Yes

Comments: No exceptions noted.

2.1.9 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.

2.1.10 Patch management process is fully developed, as specified in organization policy or standards. (NIST SP 800-53: CM-3, SI-2).

Yes

Comments: No exceptions noted.

Section 2: Configuration Management

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.

Not used.

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

Yes

Comments: No exceptions noted.

2.3.1 Is there a process for mitigating the risk introduced by those deviations?

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 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: The Department has established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines, but needs to make improvements to specific attributes as noted below.

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

No

Comments: FISMA Report: Finding No. 2, Identity and Access Management, Issue 2a – Identity and Access Management Process Needs Improvement (Modified Repeat Finding).

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

No

Comments: FISMA Report: Finding No. 2, Identity and Access Management, Issue 2a – Identity and Access Management Process Needs Improvement (Modified Repeat Finding).

3.1.3 Identifies when special access requirements (e.g., multi-factor authentication) are necessary.

Yes

Comments: No exceptions noted.

Section 3: Identity and Access Management

3.1.4 **If multi-factor authentication is in use, it is linked to the organization's PIV program where appropriate (NIST SP 800-53, IA-2).**

Yes

Comments: No exceptions noted.

3.1.5 **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.

3.1.6 **Organization has adequately 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

No exceptions noted.

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

Yes

Comments: No exceptions noted.

3.1.8 **Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users (For example: IP phones, faxes, and printers are examples of devices attached to the network that are distinguishable from desktops, laptops, or servers that have user accounts).**

Yes

Comments: No exceptions noted.

3.1.9 **Identifies all user and non-user accounts. (Refers to user accounts that are on a system. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes. They are not associated with a single user or a specific group of users.)**

Yes

Comments: No exceptions noted.

3.1.10 **Ensures that accounts are terminated or deactivated once access is no longer required.**

Yes

Comments: No exceptions noted.

Section 3: Identity and Access Management

3.1.11 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: Finding No. 2, Identity and Access Management, Issue 2b – Password Authentication Process Needs Improvement (Modified Repeat Finding). FISMA Report: Finding No. 2, Identity and Access Management, Issue 2c – Users' Logical Access Controls Not Fully Implemented.

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?

Yes

Comments: The Department has established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines, but needs to make improvements to specific attributes as noted below.

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, and OMB M-07-16, M-06-19).

No

Comments: FISMA Report: Finding No. 3, Incident Response and Reporting, Issue 3a – Incident Response and Reporting to the United States Computer Emergency Readiness Team Needs Improvement (Modified Repeat Finding).

Section 4: Incident Response and Reporting

4.1.4 When applicable, reports to law enforcement within established timeframes (NIST SP 800-61).

No

Comments: FISMA Report: Finding No. 3, Incident Response and Reporting, Issue 3b – Incident Response and Reporting to Law Enforcement Needs Improvement (Modified Repeat Finding).

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, and OMB M-07-16, M-06-19).

Yes

Comments: No exceptions noted.

4.1.6 Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.

Yes

Comments: No exceptions noted.

4.1.7 Is capable of correlating incidents.

Yes

Comments: No exceptions noted.

4.1.8 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).

Yes

Comments: No exceptions noted.

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: The Department has established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines, but needs to make improvements to specific attributes as noted below.

5.1.1 Documented policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.

No

Comments: FISMA Report: Finding No. 4, Risk Management, Issue 4a – Risk Management Program Is Not Fully Implemented (Repeat Finding).

5.1.2 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.

5.1.3 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.

5.1.4 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.

5.1.5 Has an up-to-date system inventory.

No

Comments: FISMA Report: Finding No. 4, Risk Management, Issue 4b – System Authorization Process Needs Improvement (Modified Repeat Finding).

Section 5: Risk Management

5.1.6 Categorizes information systems in accordance with government policies.

No

Comments: FISMA Report: Finding No. 4, Risk Management, Issue 4b – System Authorization Process Needs Improvement (Modified Repeat Finding).

5.1.7 Selects an appropriately tailored set of baseline security controls.

Yes

Comments: No exceptions noted.

5.1.8 Implements the 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.

5.1.9 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.

5.1.10 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.

5.1.11 Ensures information security controls are monitored on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

Yes

Comments: No exceptions noted.

Section 5: Risk Management

5.1.12 **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.

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

Yes

Comments: No exceptions noted.

5.1.14 **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.

5.1.15 **Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies. (NIST SP 800-18, SP 800-37).**

Yes

Comments: No exceptions noted.

5.1.16 **Security authorization package contains accreditation boundaries, defined in accordance with government policies, for organization information 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

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: The Department has established and is maintaining a security training program consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

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.

Yes

Comments: No exceptions noted.

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.

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.

Section 6: Security Training

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: The Department has established and is maintaining a POA&M program consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

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.

7.1.4 **Establishes and adheres to milestone remediation dates.**

Yes

Comments: No exceptions noted.

7.1.5 **Ensures resources and ownership are provided for correcting weaknesses.**

Yes

Comments: No exceptions noted.

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

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 (NIST SP 800-53, Rev. 3, Control PM-3 and 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, Rev. 3, Control 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

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?**

Yes

Comments: The Department has established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines, but needs to make improvements to specific attributes as noted below.

Section 8: Remote Access Management

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

No

Comments: FISMA Report: Finding No. 5, Remote Access Management, Issue 5i - Policy on Removable Storage Devices Needs Improvement (Repeat Finding)

8.1.2 Protects against unauthorized connections or subversion of authorized connections.

No

Comments: FISMA Report: Finding No. 5, Remote Access Management, Issue 5d - Lack of Restrictions for Virtual Private Network Client Programs on non-Government Furnished Equipment.

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

Yes

Comments: No exceptions noted.

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

Yes

Comments: No exceptions noted.

8.1.5 If applicable, multi-factor authentication is required for remote access (NIST SP 800-46, Section 2.2, Section 3.3).

No

Comments: FISMA Report: Finding No. 5, Remote Access Management, Issue 5g - Two-Factor Authentication Not Fully Implemented (Modified Repeat Finding).

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

Yes

Comments: No exceptions noted.

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

Yes

Comments: No exceptions noted.

Section 8: Remote Access Management

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

Yes

Comments: No exceptions noted.

8.1.9 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.

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

Yes

Comments: No exceptions noted.

8.1.11 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.

See Narrative for Exceptions Noted.

Comments: FISMA Report: Finding No. 5, Remote Access Management, Issue 5a - Lack of Inventory over Universal Serial Bus Storage Drives. FISMA Report: Finding No. 5, Remote Access Management, Issue 5c - FSA Continues Use of Social Security Numbers as a Primary Identifier. FISMA Report: Finding No. 5, Remote Access Management, Issue 5e - Mobile Devices with Root Access Are Allowed to Connect to the Network. FISMA Report: Finding No. 5, Remote Access Management, Issue 5f - Data Storage on Mobile and External Storage Devices Process Needs Improvement (Modified Repeat Finding). FISMA Report: Finding No. 5, Remote Access Management, Issue 5h - Data Transmission and Storage Restriction Can Be Bypassed (Repeat Finding).

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

No

Comments: FISMA Report: Finding No. 5, Remote Access Management, Issue 5b - The Department is (b)(7)(E) (b)(7)(E)

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: The Department has established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines, but needs to make improvements to specific attributes as noted below.

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 (BIA) into the analysis and strategy development efforts for the organization's Continuity of Operations Plan (COOP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) (NIST SP 800-34).

Yes

Comments: No exceptions noted.

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: Finding No. 6, Contingency Planning, Issue 6a– Contingency Plans Not Complete (Modified Repeat Finding).

9.1.4 Testing of system specific contingency plans.

No

Comments: FISMA Report: Finding No. 6, Contingency Planning, Issue 6b– 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).

Yes

Comments: No exceptions noted.

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 Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).

Yes

Comments: No exceptions noted.

9.1.10 Alternate processing sites are not subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).

Yes

Comments: No exceptions noted.

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

Yes

Comments: No exceptions noted.

9.1.12 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

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

Yes

Comments: The Department has established and is maintaining a contractor systems program consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

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 organization systems and services residing in a public 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 comply with Federal and organization guidelines (NIST SP 800-53: CA-2).(Base)**

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 organization systems and services residing in a public 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.

10.1.7 Systems that are owned or operated by contractors or entities, including organization systems and services residing in a public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.

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

Section 11: Security Capital Planning

11.1 Has the organization established a security capital planning and investment program for information security? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

Comments: The Department has established and is maintaining a security capital planning program consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

11.1.1 Documented policies and procedures to address information security in the capital planning and investment control (CPIC) process.

Yes

Comments: No exceptions noted.

11.1.2 Includes information security requirements as part of the capital planning and investment process.

Yes

Comments: No exceptions noted.

11.1.3 Establishes a discrete line item for information security in organizational programming and documentation (NIST SP 800-53: SA-2).

Yes

Comments: No exceptions noted.

Section 11: Security Capital Planning

11.1.4 Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST SP 800-53: PM-3).

Yes

Comments: No exceptions noted.

11.1.5 Ensures that information security resources are available for expenditure as planned.

Yes

Comments: No exceptions noted.

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

Not used.

Enclosure 2: Management Comments

UNITED STATES DEPARTMENT OF EDUCATION
WASHINGTON, D.C. 20202-_____

MEMORANDUM

DATE:

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

FROM: James H. Shelton, III
Deputy Secretary
Office of the Deputy Secretary

Ted Mitchell
Under Secretary
Office of the Under Secretary

SUBJECT: Draft Audit Report
Audit of the U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014
Control Number ED-OIG/A11O0001

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 Compliance with the Federal Information Security Management Act (FISMA for Fiscal Year 2014, Control Number ED-OIG/A11O0001. 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.

The Department had no findings in five of the nine areas, resulting in full compliance with the Continuous Monitoring, Security Training, Plans of Action & Milestones (POA&M), Contractor Systems, and Security Capital Planning reporting metrics. The Department has established compliant programs for enterprise-wide continuous monitoring, security awareness training, tracking and monitoring known information security weaknesses, overseeing systems operated on its behalf by contractors or other entities, and security capital planning and investments, that are consistent with FISMA requirements, Office of Management and Budget policy, and applicable National Institute of Standards and Technology guidelines. This result represents a significant improvement over FY 2013 wherein the Department had no findings in three of the eleven areas audited by OIG.

In FY 2014, the Department established a 24x7, on-premise Security Operations Center (EDSOC) that operates an integrated, enterprise-wide program, and responds to threats and vulnerabilities to the Department's information infrastructure and assets. The EDSOC utilizes a Risk Management Framework (RMF) comprised of a suite of continuous monitoring tools, and other initiatives intended to safeguard Personally Identifiable Information (PII). Also, the EDSOC provides independent verification and validation of the information security actions and activities of the

various network contractors. Additionally, the EDSOC ensures that the Department identifies, tracks, and responds appropriately to cyber incidents, vulnerabilities and threats thereby minimizing the risk and impact to the Department's mission. As we have noted in the past, the Department believes investing in continuous monitoring capabilities like the EDSOC and RMF represents an optimal strategy for improving information security given the resource and budgetary constraints faced by OCIO and FSA.

The Department has also garnered significant benefits from previous years' audits and expects that the recommendations presented in this audit will further improve 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 - Configuration Management

OIG Recommendation 1.1 - Update current configuration management policies, procedures, and plans in accordance with National Institute of Standards and Technology (NIST) and departmental guidelines.

Management Response: The Department concurs with this recommendation. The Office of the Chief Information Officer (OCIO) will update security assessment guidance and procedures to include explicit validation of configuration management standards and compliance with annual review requirements by March 30, 2015. Non-compliance will be tracked and managed via the POA&M process.

REPORTING METRIC NO.2 - Identity and Access Management

OIG Recommendation 2.1 - Update and implement policies and procedures including a NAC solution, consistent with NIST and FISMA guidelines to (1) identify all devices that are attached to the network; (2) distinguish the devices from users; and, (3) authenticate devices that are connected to the network.

Management Response: The Department concurs with this recommendation. OCIO is currently implementing an enterprise Network Access Control (NAC) solution that will allow the Department to identify all devices that are attached to the network, distinguish those devices from users, and authenticate devices that are connected to the network. As part of the NAC solution, the Department is developing a strategy and process for phasing in access control restrictions via the NAC solution to include restrictions on unauthorized or unapproved devices connecting to the network and via unrestricted ports, and validation of Government Furnished Equipment (GFE) and non-GFE security configurations for remote access. The NAC solution is currently scheduled for production by September 30, 2015, with a set of baseline configurations.

OIG Recommendation 2.2 - Develop and implement a detailed action plan on how OCIO-01, "Handbook for Information Assurance Security Policy" will be enforced to require that passwords are changed every 90 days.

Management Response: The Department concurs with this recommendation. The 90-day password change requirement has been reinforced for the users cited in the report (1840 or 28% of 6597) since the fieldwork was completed. In addition, OCIO will develop and implement an action plan by December 31, 2014, to require that passwords are changed every 90 days.

OIG Recommendation 2.3 - Restrict access rights so users of the major FSA system tested are allowed to access only authorized areas based on their pre-established roles.

Management Response: FSA concurs with the recommendation and recognizes the critical requirement of having effective access controls. FSA will initiate the access control remediation for the major system identified in this audit by March 31, 2015, and then comprehensively review all systems to ensure the proper access controls are in place by September 30, 2015. FSA will review the source code of web applications to ensure the user input is correctly validated and restrict access so users can only access authorized areas of the application based on their role. FSA will also modify the processes and procedures for design, development and maintenance of webserver applications to ensure coding practices are in compliance with NIST 800-53 Rev 4 Access Controls.

REPORTING METRIC NO.3 - Incident Response and Reporting

OIG Recommendation 3.1 - Develop and implement a detailed action plan of how existing policies and procedures will be fully implemented to ensure security incidents are reported to US-CERT within the required timeframes.

Management Response: The Department partially concurs with this recommendation. The current capabilities of the Department's Open Vulnerability Management System (OVMS) do not allow the downgrading of events after an entry is initially created. If the event is created as a category (CAT #), it retains that CAT # designation in the system until resolved. In order to validate the correct CAT #, all comments sections must be reviewed. As a result, several of the identified events were deemed not reportable, downgraded before reporting or downgraded by US-CERT. OCIO in conjunction with FSA, has conducted market research and is acquiring a new tool specifically focused on incident handling that will address this limitation. The new solution is currently scheduled be in production by June 30, 2015.

In addition, the Cybersecurity Operations US-CERT reporting guide will be modified to add a daily audit by the ED Security Operations Center (EDSOC) Management Team and a weekly audit by a government team member to ensure appropriate and timely reporting. The target completion date is December 30, 2014.

OIG Recommendation 3.2 - Develop and implement a detailed action plan of how existing policies and procedures will be fully implemented to ensure security incidents are correctly and timely reported to law enforcement.

Management Response: The Department partially concurs with this recommendation. The previous year's Corrective Action Plan (CAP) was scheduled to be, and was implemented in January 2014, with a revision in March 2014. The majority of the cited events occurred before that CAP was completed.

OCIO will meet with OIG/Technology Crimes Division (TCD) to validate the incidents that require notification. Any changes to OCIO-level existing processes will be updated by December 30, 2014. For documents that require Department-wide review and coordination, the process will be started by January 30, 2015.

Page 4

REPORTING METRIC NO.4 - Risk Management

OIG Recommendation 4.1 - Develop and implement a detailed action plan to ensure that all system authorization documentation is readily available and complies with Federal and Department standards and guidance, and take immediate action to resolve the deficiencies identified (a list of systems and applicable documentation was provided to OCIO).

Management Response: The Department partially concurs with this recommendation. OCIO has made significant efforts towards improving system security documentation and ensuring that it is readily available and complies with Federal and Department standards and guidance. OCIO has worked extensively with program offices, authorizing officials, system owners, and information system security officers through monthly meetings, targeted workshops, and one-on-one sessions in order to communicate requirements, provide templates and resources, and provide any guidance necessary. Through OCIO's concerted efforts and collaboration with program offices to properly dispose of systems, accurately characterize and document systems, and increase understanding of overall information system security requirements, the Department has experienced improvements. For the list of systems cited in the report, OCIO will ensure all documentation gaps are addressed by March 31, 2015.

OIG Recommendation 4.2 - Develop and implement controls to ensure timely re-authorizations for systems avoiding gaps in authority to operate coverage.

Management Response: The Department partially concurs with this recommendation. The Department has made significant efforts towards improving the system authorization process. Since the OIG's fieldwork was completed, the Department's system inventory has been reduced to 164 FISMA reportable systems. Of the 164 systems, 31 (19%) are currently operating with invalid Authorities To Operate (ATOs), but 16 of the systems have been through the assessment process and are currently pending final ATO signatures. OCIO is progressing with its implementation of an enterprise-wide risk management framework in accordance with NIST 800-37, and will publish guidance to address the initial and ongoing authorization of systems by June 30, 2015.

REPORTING METRIC NO.5 - Remote Access Management

OIG Recommendation 5.1 - Update its asset management policy to ensure that USB drives are recorded and maintained in a centralized asset management solution and properly disposed of upon its end-of-life.

Management Response: The Department concurs with this recommendation. The NAC solution will provide automated means to identify, inventory and control access to USB devices. The NAC solution is currently scheduled to be in production by September 30, 2015, with a set of baseline configurations.

OIG Recommendation 5.2 - Enable a NAC (b)(7)(E) capable of detecting and protecting the network against unauthorized connections.

Management Response: The Department concurs with this recommendation. The Department is currently implementing an enterprise-NAC solution that will allow the Department to identify all devices that are attached to the network, distinguish those devices from users, and authenticate devices that are connected to the network. As part of the NAC solution, the Department is developing a strategy and process for phasing in access control restrictions via the NAC solution to include restrictions on unauthorized or unapproved devices connecting to the network and via unrestricted ports, and validation of GFE and non-GFE security configurations for remote access. The NAC solution will provide an

automated means to identify, inventory and control access by USB devices. The NAC solution is currently scheduled to be in production by September 30, 2015, with a set of baseline configurations.

OIG Recommendation 5.3 - Restrict unauthorized systems from connecting to the network via a virtual private network client solution.

Management Response: The Department concurs with this recommendation. The Department is currently implementing an enterprise-NAC solution that will allow the Department to identify all devices that are attached to the network, distinguish those devices from users, and authenticate devices that are connected to the network. As part of the NAC solution, the Department is developing a strategy and process for phasing in access control restrictions via the NAC solution to include restrictions on unauthorized or unapproved devices connecting to the network and via unrestricted ports, and validation of GFE and non-GFE security configurations for remote access. Additional capabilities exist within the remote access devices that will be appropriately configured to validate and only allow access to authorized GFE. The NAC solution is currently scheduled to be in production by September 30, 2015, with a set of baseline configurations.

OIG Recommendation 5.4 - Restrict rooted mobile devices from connecting to the network and continuously monitor authorized mobile devices to validate if they have been rooted.

Management Response: The Department concurs with this recommendation. For devices managed by the Department's Enterprise Mobility Management (EMM) solution, the rooted device checks will be accomplished on a monthly basis. The Department is not aware of a technical solution to check for rooted Windows 8 mobile devices. As a result, OCIO will make a risk acceptance decision and submit the required approval documentation by December 31, 2014.

OIG Recommendation 5.5 - Enable full disk encryption on mobile devices and external storage devices that store Departmental data.

Management Response: The Department concurs with this recommendation. For mobile devices (laptops), full-disk encryption is fully deployed on all devices. For external mass storage (USB flash drives and external hard drives), OCIO is piloting a solution to encrypt those devices.
In FY14, OCIO initiated the implementation of an enterprise-wide Data Loss Prevention (DLP) capability to provide greater protection of sensitive government, financial, and privacy data and allow for more visibility into incidents where information is either maliciously or inadvertently infiltrated from Department networks. In FY15, the Department will expand the implementation to include automated response actions such as enforcing the encryption of sensitive data prior to saving to an external storage device and prior to transmitting via email. While full-disk encryption on mobile and external storage devices is a robust technical control, the ability to enforce encryption of sensitive data prior to saving to an external device sufficiently minimizes departmental risk and provides an adequate layer of protection for sensitive data. The DLP solution is currently scheduled to be in production by September 30, 2015.

OIG Recommendation 5.6 - Enable dual-authentication via all external connections to the G5 application.

Management Response: The Department concurs with this recommendation. In FY14, the Department completed the implementation of an enterprise Single Sign On (eSSO) solution that allows internal Personal Identification Verification (PIV) cardholders to logon to Department systems using a PIV card and Personal Identification Number (PIN). The Grants Management System (G5) moved behind the eSSO solution. In addition, the Department is in the process of transitioning from the Two Factor

Authentication (TFA) Symantec hard token solution to the Symantec soft token VIP solution for remote access for internal users and the potential use of the soft tokens for external users. OCIO, in conjunction with FSA, will determine the feasibility of transitioning to the solution for external users by February 28, 2015.

OIG Recommendation 5.7 - Eliminate the use of SSNs as the primary identifier when authenticating onto FSA web sites by requiring the user to create a unique identifier for account authentication.

Management Response: FSA concurs with the recommendation. FSA fully appreciates the critical need to ensure the security of PII and recognizes the threat the use of SSNs for account access could pose. FSA has been developing a new access control capability for the 70 million non-privileged users (students and borrowers) with strong logon and verification capabilities. The Person Authentication Service (PAS) removes the use of PII, specifically the SSN, from the authorization process and thus reduces the risk. This new system will be implemented for users by June 30, 2015, and utilized for access to Free Application for Federal Student Aid (FAFSA) and National Student Loan Data System (NSLDS).

REPORTING METRIC NO. 6 - Contingency Planning

OIG Recommendation 6.1 - Review and update information system contingency plans for the six systems that have elements missing to ensure that all the contingency planning elements are included as required by NIST guidelines and Departmental guidance.

Management Response: The Department concurs with this recommendation. OCIO will review the information system contingency plans for the six systems that have elements missing to ensure that all the contingency planning elements are included as required by NIST guidelines and departmental guidance by March 30, 2015. The deficiencies will result in findings issued against the respective information system and remediation tracked via the POA&M process.

OIG Recommendation 6.2 - Perform and document contingency plan test results for the nine systems in question as required by NIST guidelines and Departmental procedures.

Management Response: The Department concurs with this recommendation. OCIO will review the information system contingency plan test results for the nine systems identified by March 30, 2015. The deficiencies will result in findings issued against the respective information system and remediation tracked via the POA&M process.

OIG Recommendation 6.3 - Develop and implement a detailed action plan to ensure Information System Security Officers and/or system owners are performing and documenting annual contingency plan testing for all Departmental systems as required by NIST guidelines and departmental procedures.

Management Response: The Department concurs with this recommendation. OCIO will develop and implement a detailed action plan to ensure Information System Security Officers and/or system owners are performing and documenting annual contingency plan testing for all departmental systems by March 30, 2015.

Page 7

REPORTING METRIC NO. 7 - Implementation of Corrective Action Plans

OIG Recommendation 7.1 - A verification of completed corrective actions is performed prior to entry into AARTS to ensure that recommendations are correctly addressed.

Management Response: The Department concurs with this recommendation. OCIO and FSA will verify completed corrective actions are performed prior to entry into AARTS to ensure that recommendations are correctly addressed. Incomplete actions will be noted and returned to the area of responsibility for further action until completed. The target completion date is February 28, 2015.

OIG Recommendation 7.2 - Completion dates for corrective action plans are revised appropriately and that justification is provided to support revised completion dates.

Management Response: The Department concurs with this recommendation. OCIO and FSA have developed an escalation and oversight process for all revisions to completion dates. The process will continue to be enforced for all existing and new corrective action plans.

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 Chief Information Officer Danny Harris at (202) 245-6259.

cc: Danny Harris
James Runcie
Jerry Williams
Steve Grewal