The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013

FINAL AUDIT REPORT

ED-OIG/A11N0001
November 2013

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

Abbreviations and Acronyms Used in this Report

CAT	Category
CCV	Cybersecurity Capability Validation
CSA	Continuous Security Authorization
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
IG	Inspector General
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OVMS	Operational Vulnerability Management Solution
POA&M	Plan of Action and Milestones
SP	Special Publication
TIC	Trusted Internet Connection
VDC	Virtual Data Center
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team

UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Information Technology Audit Division

November 13, 2013

Memorandum

TO: Danny A. Harris, PhD.
Chief Information Officer
Office of the Chief Information Officer

Jerry E. Williams
Chief Information Officer
Federal Student Aid

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 2013
Control Number ED-OIG/A11N0001

Attached is the subject final audit report that covers the results of our review of the Department's compliance with the Federal Information Security Management Act for fiscal year 2013. An electronic copy has been provided to your audit liaison officer. We received your comments on the findings and recommendations in our draft report.

Corrective actions proposed (resolution phase) and implemented (closure phase) by your office will be monitored and tracked through the Department's Audit Accountability and Resolution Tracking System. Department 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 6 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 us during this review. If you have any questions, please call Joseph Maranto at 202-245-7044.

Enclosure

Cc: Steve Grewal, Director, Information Assurance Services
Dana Stanard, Audit Liaison, OCIO
Mark Love, Audit Liaison, Federal Student Aid
Linda Wilbanks, PhD, Chief Information Security Officer, Federal Student Aid
Bucky Methfessel, Senior Counsel for Information & Technology, Office of the General Counsel
Charles Laster, Post Audit Group, Office of Chief Financial Officer
L'Wanda Rosemond, AARTS Administrator, OIG

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 metrics that the Department of Homeland Security (DHS) provided for the annual FISMA review. The review was designed to assess the status of the Department's security posture for 11 identified control areas for fiscal year 2013. The control areas 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.

For the fiscal year 2013 FISMA review, DHS's framework required us to evaluate the information technology processes, policies, and procedures that the Department had already documented, implemented, and was monitoring. Although the Department has many planned activities that may improve its security posture in the future, we could not evaluate those planned activities because they were not fully operational at the time of our review. As part of the FISMA review, the OIG evaluated Department systems, contractors, annual self-assessments, policies, procedures, various OIG audit reports, and other Federal agency reports issued throughout the year. During the work plan process, the Office of the Deputy Secretary requested that the OIG review key aspects of Federal information system cyber security. Specifically, they requested that we focus on the Department's compliance with Federal guidelines in the areas of continuous monitoring, personal identification verification, and trusted internet connections. We also conducted vulnerability and penetration (both internal and external) testing for Federal Student Aid's Virtual Data Center located in Plano, Texas. The results of this testing are summarized in this report. We also observed a disaster recovery exercise at the Virtual Data Center recovery site in Philadelphia, Pennsylvania.

Our objective was to determine whether the Department and Federal Student Aid's overall information technology 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. Specifically, we 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]

We found that the Department has made progress in remediating issues identified in previous FISMA reviews. Specifically, we found the Department was compliant in 4 of the 11 reporting metrics. However, we identified findings in seven of the reporting metrics. These findings included issues in critical areas such as (1) configuration management, (2) identity and access management, (3) incident response and reporting, (4) risk management, (5) security training, (6) remote access management, and (7) contingency planning. Also, the findings in seven of the

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

reporting metrics contained repeat or modified repeat findings from OIG reports issued from fiscal years 2010 through 2012.[2] In addition, we identified a finding in the Department's Trusted Internet Connections initiative. We answered the questions in the DHS metrics template, based on our audit work, which will become the CyberScope FISMA Report as shown in Enclosure 1.

The OIG is concerned that the Department has not assigned proper priority to remediating outstanding issues from previous audit reports. In addition to 7 of the 11 reporting metrics containing repeat or modified repeat findings from this review and the previous 3 years, we have cited similar findings in the FY 2011 and 2012 OIG FISMA reports. Although the Department takes corrective action on the findings identified with each report, the OIG is concerned the Department does not take the appropriate action to correct the identified issues systematically across the infrastructure, which leads again to repeat and modified repeat findings.

In addition to recommendations we made in the Fiscal Year 2012 FISMA report, we are making 23 new recommendations to the Office of the Chief Information Officer to assist the Department in establishing and sustaining an effective information security program—one that complies with requirements of FISMA, the Office of Management and Budget, and the National Institute of Standards and Technology requirements.

OCIO concurred with 21of the 23 recommendations and partially concurred with the remaining 2 recommendations (8.2 and 8.3). We summarize and respond to specific comments in the "Audit Results" section of the audit report. We considered OCIO's comments but did not revise our findings or recommendations.

[2] Repeat findings are current report findings with the same or similar conditions to those contained in prior OIG reports.

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 standards and guidelines, including:

- standards for Federal agencies to use to categorize all information and information systems collected or maintained by or on behalf of each agency based on providing appropriate levels of information security according to a range of risk levels;
- guidelines recommending the types of information and information systems to be included in each category; and
- minimum information security requirements (management, operational, and technical controls) for information and information systems in each such category.

FISMA supplements information security requirements established in the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Clinger-Cohen Act of 1996. FISMA consolidated these separate requirements and guidance into an overall framework for managing information security. It established new annual reviews, independent evaluation, and reporting requirements to ensure that agencies implemented FISMA. It also established how the Office of Management and Budget (OMB) and Congress would oversee information technology (IT) security.

Under various national security and homeland security Presidential directives, the Department of Homeland Security (DHS) oversees critical infrastructure protection, operates the United States Computer Emergency Response Team, oversees implementation of the Trusted Internet Connections initiative, and takes other actions to help secure both the Federal civilian government systems and the private sector. OMB is responsible for submitting the annual FISMA report to Congress, for developing and approving the cyber security portions of the President's Budget, and for overseeing agencies' use of funds. DHS has primary responsibility within the Executive Branch for the operational aspects of Federal agency cyber security with respect to the Federal information systems that fall within FISMA.

DHS updated the Inspector General (IG) reporting metrics for fiscal year (FY) 2013 to better align with the Chief Information Officer's metrics, allowing the IGs to determine the progress of the control areas on which the Chief Information Officers report. DHS introduced this change to ensure that IGs move towards measuring progress on the control area rather than simply

measuring an agency's compliance. The E-Government Act also assigned specific responsibilities to OMB, agency heads, Chief Information Officers, and IGs. OMB is responsible for establishing and overseeing policies, standards, and guidelines for information security. The responsibilities include the authority to approve agencies' information security programs. 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. The evaluations are to be performed by the agency's IG or an independent evaluator, and the results of these evaluations are to be reported to OMB. Beginning in FY 2009, OMB required Federal agencies to submit FISMA reporting through the OMB Web portal, CyberScope.

As of July 2013, the Department had spent a total of $623 million on IT investments for FY 2013. The Department budgeted $9.2 million for FY 2013 on IT security and FISMA compliance costs (1.5 percent of the total IT budget).

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 communication devices, voice mail, and the Department's laptops and workstations.

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

The contractor 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 EDUCATE subsystems include the EDUCATE Network Infrastructure System, the EDUCATE Mass Storage System, the EDUCATE Security Operations Center (EDSOC), the Department of Education's Central Automated Processing System, the EDUCATE Data Center Information System, and the Case Activity Management System, as well as the wide-area and local-area network hardware consisting of network servers, routers, switches, and external firewalls.

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 agency's Chief Information Officer 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 common operating environment called the Virtual Data Center (VDC) to improve interoperability and reduce costs. The Department considers the VDC to be a general support system. 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. The VDC serves as the host facility for FSA systems that process student financial aid applications (grants, loans, and work-study), provide schools and lenders with eligibility determinations, and support payments from and repayment to lenders.

The Department's systems contain or protect large amounts of confidential information (personal records, financial information, and other personally identifiable information) and perform vital organizational functions. Unauthorized individuals might target the systems by exploitation, but the systems could also be targeted by trusted individuals inside the Department, as well as by Department contractors. 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 data, as well as the potential that sensitive data may be released, used, or modified.

AUDIT RESULTS

In November 2012, DHS prepared the IG reporting metrics, or controls areas, for the FY 2013 FISMA review. The intent of the FY 2013 reporting metrics was to determine the Department's progress in the control areas from the previous year's reporting. The 11 controls areas for the FY 2013 FISMA review included Continuous Monitoring, Configuration Management, Identity and Access Management, Incident Response and Reporting, Risk Management, Security Training, Plan of Action and Milestones, Remote Access Management, Contingency Planning, Contractor Systems, and Security Capital Planning.

We found that the Department has made progress in remediating issues identified in previous FISMA reviews. Specifically, we found the Department to be compliant in 4 of the 11 reporting metrics. However, we identified findings in seven of the reporting metrics. The findings in seven of the reporting metrics contained repeat findings from reports issued from FY 2010 through FY 2012. In addition, we identified a finding in the Department's Trusted Internet Connections (TIC) initiative.

Several prior reports had similar or repeat findings to this year's audit fieldwork. These reports include:

- "The U.S. Department of Education's Compliance with the Federal Information Security Management Act for Fiscal Year 2012," November 2012 (ED-OIG/A11M0003);
- "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 2011," October 2011 (ED-OIG/A11L0003);
- "Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE)," September 2011 (ED-OIG/A11L0001);
- "Incident Response and Reporting Procedures," June 2011 (Investigative Program Advisory Report ED-OIG/L21L0001);
- "Weaknesses in the Process for Handling Compromised Privileged Accounts," September 2010 (Investigative Program Advisory Report ED-OIG/L21K0002); and
- "Security Controls for Data Protection over the Virtual Data Center," September 2010 (ED-OIG/A11J0006)

In its response to our draft report, OCIO concurred or partially concurred with the findings and recommendations in the report. We summarized and responded to specific comments in the "Findings" section of the audit report. We considered OCIO's comments but did not revise our findings or recommendations. OCIO's response is included as Enclosure 3 to this audit report.

Management Response to the Overall Report

OCIO stated that it sincerely values the FISMA audit activity the OIG conducted and appreciates the benefits of the collaborative relationship between the OIG and the Department, formed through years of partnering and the sharing of mutual goals and objectives.

OCIO stated the Department has benefitted from previous years' audits and expects that the recommendations presented in this current audit will further improve the information security program by strengthening the associated management, technical, and operational security controls. OCIO will address each finding and recommendation as stipulated in the plan provided and as agreed on by the OIG.

REPORTING METRIC NO. 1—Continuous Monitoring Management

FISMA FY 2013 Audit Results

The Department complied with this reporting metric. The OCIO and FSA established continuous monitoring programs that assessed the security state of information systems in the Department's two distinct environments, EDUCATE and VDC, respectively, that are consistent with OMB policy, FISMA requirements, and applicable NIST guidelines. Both the OCIO and FSA adopted and were using several automated scanning and detection tools to collect, analyze, and report on security-related risks, issues, and threats to the Department. Also, they both used the Operational Vulnerability Management Solution (OVMS) for tracking and managing vulnerabilities where remediation actions had not been taken within 30 days. In addition, OCIO and FSA used a change detection tool that formulated reports identifying current vulnerabilities. These reports were used by their respective System Security Officer/Information System Security Officers (ISSO) in monitoring corrective actions.

We found that the Department's continuous monitoring program was consistent with the reporting metrics and included the following attributes:

- documented policies and procedures for continuous monitoring;
- documented strategy and plans for continuous monitoring;
- ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on approved continuous monitoring plans; and
- security status reports for authorizing officials and other key system officials, including updates to security plans, security assessment reports, and plans of action and milestones (POA&M).

REPORTING METRIC NO. 2—Configuration Management

FISMA FY 2013 Audit Results

The Department did not fully comply with this reporting metric.

Issue 2a. Configuration Management Plans Were Not Consistently Developed (Modified Repeat Finding)

The Department's configuration management plans were not consistently developed to include complete systems' baseline configurations as required in NIST and Departmental guidance.[4] Based on our review of the configuration management plans of the 16 systems we sampled, we found that 3 systems did not have complete system baseline configurations documented. Specifically, the Department did not define the systems' software and hardware in their respective configuration management plans for either: (1) the VDC, (2) the National Student Loan Database System, or (3) the OVMS.

NIST Special Publication (SP) 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," CM-2 Baseline Configuration, states the organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system. OCIO-11, "Handbook for IT Security Configuration Management Planning Procedures," states the first step of the configuration control process is to establish the System Configuration Baseline that identifies servers, workstations, and software applications that are currently being used in the production environment and the specific configuration settings for each. The Department was not consistently following the procedures as stipulated in NIST SP 800-53, Revision 3 and the OCIO-11 Handbook when establishing the system configuration baseline, which identifies the current design and functionality of a general support system or major application.

Without complete system configuration management plans, the Department may not be able to track configuration changes to systems. Patches may not be easily implemented if software and hardware controls are not documented in the systems' baseline configuration. As a result, the Department may not be able verify changes made against the initial baseline configurations.

Issue 2b. Patch Management Program Needs Improvement

The Department had not established and implemented formal, enterprise-wide patch management policy and procedures consistent with NIST requirements. Although the Department relied on Dell's patch management policy and procedures for the past 3 years, the absence of a Department issued policy and procedures does not provide assurance that the current patch management guidance incorporates federal requirements such as NIST SP 800-53, Revision 3, Configuration Management-3, "Configuration Change Control and System," that requires agencies to timely implement configuration control changes and to promptly install security-relevant software updates. Without effective patch management policies and procedures that ensure security patches are tested and timely installed, the Department increases the risks that unauthorized activities may occur and increases the potential that sensitive Department data may be released, used, or modified.

In September 2013, OCIO issued the enterprise-wide vulnerability and patch management guidance in response to prior FISMA audit recommendations. Although this addresses our

[4] 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."

concern regarding guidance, since it was issued after fieldwork was concluded, we could not adequately determine if the Department has fully implemented this guidance. Therefore, we will evaluate the implementation of this guidance during our FY 2014 FISMA review.

Issue 2c. Patch Management Process Needs Improvement (Modified Repeat Finding)

FSA has not implemented sufficient monitoring and oversight controls enterprise-wide to ensure recommendations from prior OIG reports were implemented to address the patch management control deficiencies. Although FSA uses several automated scanning and detection tools to collect, analyze, and report on security-related issues and threats to its computing environment, the OIG identified numerous vulnerabilities that still existed. For example, from April 2009 through July 2011, we identified 105 (b) (7)(E) Patch Updates[5] that were missing. Deficiencies such as these have been identified in prior audit reports from FY 2010 through FY 2012.[6] The OIG performed a vulnerability assessment of the Department's data center environment and identified major vulnerability trends in network configuration. Detailed information on the vulnerabilities was provided to FSA for remediation.

NIST SP 800-53, Revision 3,"Recommended Security Controls for Federal Information Systems and Organizations," SI-2 Flaw Remediation, requires organizations to (1) identify, report, and correct information system flaws; (2) test software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and (3) incorporate flaw remediation into the organizational configuration management process. FSA did not adequately monitor or establish sufficient reporting requirements to ensure Dell updated the systems with vendor-supplied security patches and to measure Dell's progress on remediating known vulnerabilities. Additionally, despite the OIG reporting the same conditions from FY 2010 through FY 2012, OCIO and FSA had not established a proactive enterprise-wide solution to patch all Department systems.

Without ensuring that patches are installed in a timely manner, OCIO exposes the Department to unauthorized and unauthenticated access to the Department's network and data and hinders its ability to audit and track users' activities within the data center. The lack of suitable controls increases the potential of unauthorized changes to the operating system and application code, which could lead to the theft, destruction, or misuse of sensitive data and Departmental assets. Further, a proactive process should include ensuring hardware operating systems are updated with security patches as recommended by the software vendor and are configured correctly to prevent or detect unauthorized activities such as theft, destruction, and misuse of agency data both from internal and external threats.

In September 2013, FSA stated that for certain vulnerabilities identified during the OIG's assessment, Risk Analysis Forms were in place that could addresses specific deficiencies. Although FSA provided the OIG its Risk Analysis Form[7] information to address the

[5] (b) (7)(E) Patch Updates resolve vulnerabilities in the (b) (7)(E) Server.
[6] A11J0006 FY2010 VDC Final Report, Issue 1c; A11L0001 FY2011 EDUCATE Report Finding 3; A11M0002 FY2012 EDCAPS Final Report Finding 2.
[7] A Department of Education Risk Analysis Form is an internal form Department officials use to justify and document risk acceptance for noncompliance, weaknesses, vulnerabilities, associated risk level (per NIST SP 800-30), and countermeasures posed to identified systems. The form identifies the responsible parties, description of the risk (as it relates to NIST SP 800-53), and signatures and approvals from authorized officials.

vulnerabilities identified, since fieldwork had ended and OIG was in the reporting process, we were not able to analyze the information for this FISMA cycle. Therefore, the analysis will be performed for the FY 2014 FISMA review.

Issue 2d. Controls for Identifying and Resolving Configuration Management Vulnerabilities Need Improvement (Modified Repeat Finding)

OCIO and FSA's implementation and management of the technical security architecture supporting the Department's enterprise network needs strengthening to more effectively restrict unauthorized access to information resources, particularly from within the security perimeter domain. The deficiencies have been identified in prior audit reports from FY 2010 through FY 2012.[8] The OIG performed a vulnerability assessment of the data center environment and identified major vulnerability trends in network configuration. Detailed information on the vulnerabilities was provided to FSA for remediation.

FSA did not implement remedial actions to address previously identified security weaknesses and did not establish a proactive enterprise-wide process to fix the vulnerabilities identified during previous audits in accordance with NIST SP 800-53, Revision 3,"Recommended Security Controls for Federal Information Systems and Organizations," SI-2 Flaw Remediation. Poor system configuration management practices increase the potential for unauthorized activities to occur without being detected and could lead to potential theft, destruction, or misuse of agency data from both internal and external threats.

As cited in Issue 2c., FSA will rely on Risk Analysis Forms to address certain vulnerabilities that will be analyzed during OIG's FY 2014 FISMA review.

Issue 2e. Access Switch Port Security Needs Improvement

OCIO still had not established access switch port security for the switches within the enterprise network infrastructure, nor did it disable unused switch port connections.[9] During June 2013, we tested switch port security by successfully connecting a rogue computer to one Departmental local-area network connection at the Department's headquarters office. During the test, OIG testers were able to gain a network internet protocol address and scanned the network by using a security scanner to obtain information of online systems. The information obtained allowed OIG users to access internal network resources and gather additional information (extracted from online printers) which could be used in a possible social engineering attack. In addition, information obtained from printers allowed users to see "header information" of documents sent to printers and contacts stored on the printers; and since the print servers were not password protected, an attacker could easily change settings or lock the administrators out. We scanned the network using NIST and the "Defense Information Systems Agency Network Security Checklist (CISCO Layer 2 Switch)" which requires that information systems have all access switch ports secured.[10] This issue was originally identified during our FY 2011 FISMA audit and was cited as a repeat finding in our FY 2012 FISMA report.

[8] ED-OIG/A11J0006, FY 2010 VDC Final Report; A11L0001, FY 2011 EDUCATE Report; and A11M0002, FY 2012 EDCAPS Final Report.

[9] Switch port security consists of software settings that control authorized access from the ports to the switches.

[10] NIST SP 800-53, Revision 3, CM-6 Configuration Settings, SI-6 Security Functionality Verification, System and Communications Protection (SC)-7 Boundary Protection, SC-20 Secure Name/Address Resolution Service,

After completing our fieldwork, we were informed by OCIO that corrective action was implemented for this issue. OCIO provided a memorandum, dated August 2013, issued by the Director, Information Assurance Services, requiring that Dell shut down or disable unused and unassigned switch port connections by September 1, 2013. The memorandum also required Dell to submit a Risk Acceptance Form identifying all unassigned and unused switch port connections on the Department's networks that cannot be disabled or shut down. Because implementation was completed after OIG fieldwork had ended, we were not able to validate the corrective action. Therefore, validation testing for this corrective action will be conducted during our FY 2014 FISMA work.

Final Reports Issued From FY 2010 Through 2012 Relating to Configuration Management

In addition to the FY 2012 FISMA audit, the OIG has consistently reported configuration management issues in audits dating back to FY 2010.[11]

Recommendations

We recommend that FSA:

2.1 Ensure all Department system configuration management plans are prepared uniformly to include system configuration baselines and to document system upgrades and additions to software and hardware components when applicable.

2.2 Require Dell to comply with the patch testing and implementation procedures documented in the OCIO-01, "Handbook for Information Assurance Security Policy."

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

2.4 Establish reporting procedures to monitor Dell's monthly progress to ensure identified vulnerabilities are fixed within the established timelines.

We recommend that OCIO:

2.5 Immediately correct or mitigate the vulnerabilities with the (b) (7)(E) [redacted] and EDUCATE web applications identified during the vulnerability assessment.

Management Response

OCIO concurred with the recommendations.

Incidence Response-6 Incident Reporting, Access Controls-4 Information Flow Enforcement, Audit and Accountability (AU)-6 Audit Review, Analysis, and Reporting, Planning (PL)-2 System Security Plan.
[11] See reports ED-OIG/A11J0006, A11L0001, A11L0003, A11M0002, and A11M0003.

REPORTING METRIC NO. 3—Identity and Access Management

FISMA FY 2013 Audit Results

The Department did not fully comply with this reporting metric.

Issue 3a. Identity Access and Management Process Needs Improvement (Modified Repeat Finding)

OCIO had not fully developed processes for identity and access management. Specifically, we found that the OCIO had not fully established policies and procedures to (b) (7)(E) NIST SP 800-53, Revision 3, IA-2, "User Identification and Authentication," and IA-3, "Device Identification and Authentication," require that information systems uniquely identify and authenticate users and specific devices before establishing a connection. OCIO is still in the process of finalizing its study on a Network Access Control solution. OCIO is updating its policy requirements for an enterprise-wide Network Access Control solution and implementing procedures for identity and access management in response to the OIG's recommendations from the FY 2011 and FY 2012 FISMA reports.

Although the OCIO has not fully implemented policies and procedures, the OIG noted that it had taken several actions to address the previous years' recommendations. Particularly, the OCIO has added steps to its identity and access management policies 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 and NIST guidance.

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 unauthorized transactions or functions. Consequently, the Department's information is vulnerable to attacks that could lead to a loss of confidentiality resulting from unauthorized access to data. Further, there is increased risk that unauthorized activities or excessive use of system resources could reduce the reliability and integrity of Department systems and data, as well as the potential that sensitive data may be released, used, or modified.

Issue 3b. Password Authentication Process Needs Improvement

The Department did not consistently follow and enforce the required Federal and Departmental guidelines requiring users to update their network passwords. OCIO officials explained that the Department's Active Directory is configured to automatically notify and prompt users to change their network passwords after 90 days.[12] 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 from the Active Directory and the date of all users' last password change. Per our review of the provided data, we found that:

[12] According to OCIO officials, EDUCATE ED.GOV Active Directory Domain environment is used by the Department to track and account for users last logon activities and their current status.

- about 1,200 of 9,523 users did not change their passwords for more than 90 days as required;
- 165 users did not change their password for more than 600 days; and
- 5 users were able to access the network despite expired passwords (3 user accounts had been expired for 2 years, and 2 user accounts for a year)

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. In addition, 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.

The Department did not enforce the password change requirement by locking out users who did not change their passwords. 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.[13] Further, password policies help to minimize risk associated with losing older backups to an attacker, and decrease the potential for unauthorized users to obtain and use an account password.

Issue 3c. Users' Account Deactivation Process Needs Improvement (Modified Repeat Finding)

The Department did not consistently and effectively ensure that user accounts inactive for 90 days were disabled, as required by Federal and Departmental guidelines. The Department's "Logical Access Control Guidance" states that accounts must be configured to be disabled after 90 days of inactivity. Particularly, users not logged in to the system for 90 or more days are considered inactive and should be disabled. According to the OCIO officials, accounts are reviewed and tracked on a monthly basis, with results captured in a 90-day report. As part of the active directory inactive user object cleanup, the Department uses the 90-Day Report to track and deactivate users who do not log into the system for 90 or more days. To validate whether the Department was consistently and effectively disabling user accounts as required, we requested the most recent 90-day reports at the time. We found that as of May 2013, 824 of the 896 inactive user accounts were not being disabled as required.

NIST SP 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," AC-2 Account Management, requires agencies to (1) identify authorized users of the information system, establish conditions for group membership, and specify access authorizations (that is, privileges) and other attributes (as required) for each account; (2) establish, activate, modify, disable, and remove information system accounts in accordance

[13] Attackers may attempt to determine weak passwords and recover passwords from password hashes through two types of techniques: guessing and cracking. Guessing involves repeatedly attempting to authenticate using default passwords, dictionary words, and other possible passwords. Cracking is the process of an attacker recovering cryptographic password hashes and using various analysis methods to attempt to identify a character string that will produce one of these hashes, thereby being the equivalent of the password to the targeted system.

with organization-defined procedures or conditions; and (3) monitor the use of information system accounts.

Failure to properly disable the user accounts in a timely manner could lead to sharing of credentials or continued access from unauthorized users. This could lead to data leakage, exposure, and ultimately to fraud, waste, and abuse.

Final Reports Issued From FY 2011 Through 2012 Relating to Identity and Access Management

The current identity and access management condition was also identified during our FY 2012 FISMA audit. In addition to the FY 2012 FISMA audit, the OIG reported identity and access management issues in a previous audit for FY 2011.[14]

Recommendations

We recommend that OCIO:

3.1 Ensure that OCIO-01, "Handbook for Information Assurance Security Policy" is enforced to require that passwords are changed every 90 days.

3.2 Enforce Departmental procedures to disable user accounts that have not been accessed for 90 days or longer, in accordance with FISMA and applicable regulations, guidance, and standards established in NIST guidelines.

We are not making additional recommendations because a corrective action to address a recommendation contained in the FY 2011 FISMA report was still outstanding.

Management Response

OCIO concurred with the recommendations.

REPORTING METRIC NO. 4—Incident Response and Reporting

FISMA FY 2013 Audit Results

The Department did not fully comply with this reporting metric.

Issue 4a. Incident Response and Reporting to the United States Computer Emergency Readiness Team Needs Improvement (Modified Repeat Finding)

The Department's incident response program needs improvement to ensure timely reporting of 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

[14] See reports ED-OIG/A11L0001and A11M0003.

relies on the US-CERT standards category listings and timelines for incident response reporting. To determine whether OCIO complied with reporting security incidents to US-CERT, we judgmentally sampled incident tickets from OVMS from October 1, 2012, through March 20, 2013. Of our sample of 22 incidents, 5 incidents (23 percent) were not reported to US-CERT within the required reporting timeframes. The following table presents the results of our tests.

Category	Sampled	Not in Compliance with US-CERT Reporting	Percentage Not in Compliance
CAT 1: unauthorized access; should be reported within 1 hour	6	2	33
CAT 2: denial of service; should be reported within 2 hours if the successful attack is ongoing and the agency is unable to mitigate	3	1	33
CAT 3: malicious code; should be reported daily, or within 1 hour if it is widespread across the agency	5	1	20
CAT 4: improper usage (violation of security policy); should be reported weekly	6	0	0
CAT 5: scans, probes, or attempted access; should be reported monthly	2	1	50
Total	**22**	**5**	**23**

- Two of the six Category (CAT) 1 incidents tested in OVMS were not reported to US-CERT within 1 hour of discovery or detection, as required by US-CERT Federal Incident Reporting Guidelines. Specifically, one incident was not reported until about 23 hours after discovery or detection, and the other incident was not reported until 3 hours after discovery or detection.
- One of the three CAT 2 incidents tested in OVMS was not reported to US-CERT within 2 hours of discovery or detection, as required by US-CERT Federal Incident Reporting Guidelines. Specifically, the incident was not reported until 3.5 days after discovery or detection.
- One of the five CAT 3 incidents tested in OVMS was not reported to US-CERT within 1 day of discovery or detection, as required by US-CERT Federal Incident Reporting Guidelines. Specifically, the incident was not reported until 5 days after the discovery or detection.
- One of the two CAT 5 incidents tested in OVMS was not reported to US-CERT within 1 month of discovery or detection, as required by US-CERT Federal Incident Reporting Guidelines. Specifically, the incident was not reported until 2.5 months after the discovery or detection.

OCIO did not adequately follow its policies and procedures for reporting security incidents within the required US-CERT timeframes. In addition, OCIO did not appoint a secondary point

of contact with US-CERT as required by NIST. According to OCIO-14, "Handbook for Information Security Incident Response and Reporting Procedures," only the Department's Computer Incident Response Capability Coordinator is responsible for reporting all incidents to external entities, including US-CERT. In accordance with NIST SP 800-61, Revision 2, each agency must designate a primary and secondary point of contact with US-CERT. FISMA requires Federal agencies to report incidents to US-CERT in a timely manner. Delays in incident reporting could hamper US-CERT's ability to properly analyze the information to identify trends and precursors of attacks. US-CERT augments the efforts of Federal civilian agencies by serving as a focal point for dealing with incidents. It is critical to notify US-CERT within the established timeframes so it can effectively assist in coordinating communications with the other agencies in handling incident response and reporting.

Issue 4b. Incident Response and Reporting to Law Enforcement Needs Improvement

The Department's incident response program needs improvement to ensure security incidents are reported to law enforcement in accordance with organizational procedures. 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 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).

To determine whether the Department reported incidents to law enforcement correctly and timely, we judgmentally sampled incident tickets from OVMS from October 1, 2012 to March 20, 2013. Based on our sample of 22 incidents, 14 incidents (64 percent) were either not timely reported or not reported at all to the OIG. Our tests disclosed the following:

US-CERT Category	Sampled	Not in Compliance with Law Enforcement Reporting	Percentage Not in Compliance
CAT 1	6	5	83
CAT 2	3	1	33
CAT 3	5	1	20
CAT 4	6	6	100
CAT 5	2	1	50
Total	**22**	**14**	**64**

- Five of the six CAT 1 incidents tested in OVMS were not reported to law enforcement in accordance with OCIO-14. Specifically, four incidents included possible exposure of personally identifiable information, which should have been reported to the OIG. These incidents included lost or stolen mobile devices, a lost Universal Serial Bus (USB) storage device, a missing laptop, and unauthorized access of a Department's IT system and electronic data.
- One of the three CAT 2 incidents tested in OVMS was not timely reported to law enforcement in accordance with OCIO-14. Specifically, the incident was not reported to the OIG until about 6 days after discovery/detection. [15]
- One of the five CAT 3 incidents tested in OVMS was not reported to law enforcement in accordance with OCIO-14. Specifically, the incident was not reported to the OIG until about 6 days after discovery/detection.
- All six of the CAT 4 incidents tested in OVMS were not reported to law enforcement in accordance with OCIO-14. Specifically, all six incidents were events that included possible exposure of personally identifiable information which should have been reported to OIG.
- One of the two CAT 5 incidents tested in OVMS was not reported to law enforcement in accordance with OCIO-14. Specifically, the incident included an unauthorized access attempt of a Department's IT system that should have been reported to OIG.

The OCIO did not follow its policies and procedures for reporting applicable security incidents to the OIG. One reason that many security-related incidents do not result in convictions is that organizations do not properly contact law enforcement. The failure to provide law enforcement timely incident reports may directly impede criminal investigative activities. 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 be unable to make important connections to ongoing cases and decisions about initiating new cases.

Final Reports Issued From FY 2011 Through 2012 Relating to Incident Response and Reporting

Multiple reports were issued that identified findings relating to incident response, including the FY 2011 and FY 2012 FISMA reports and the FY 2011 EDUCATE report.[16] Specifically, OCIO was not in compliance with NIST requirements to report security incidents to the US-CERT within required timeframes. Further, OCIO did not timely resolve security incidents to prevent further damage. In addition to the EDUCATE audit, the OIG's Technology Crimes Division reported in 2011 that investigations of potential computer crimes in previous years identified problems with how the Department handled computer security incidents. Specifically, the Department did not detect, report, or respond to incidents in accordance with the OCIO-14, "Handbook for Information Security Incident Response and Reporting Procedures," which is based on Federal guidelines and industry best practices.

[15] Although NIST SP 800-61, Revision 2, and OCIO-14 do not specify a specific timeline for reporting applicable incidents to law enforcement, we believe that not reporting an incident until 6 days after its detection or discovery is not "timely" reporting because crucial evidence may be lost and the investigation impeded because of the delay.
[16] See reports ED-OIG/A11L0001, A11L0003, and A11M0003. In addition, the results of the FY 2011 EDUCATE report were cited as support in our FY 2012 FISMA report.

Recommendations

We recommend that OCIO:

4.1 Follow existing policies and procedures to ensure security incidents are reported to US-CERT within the required timeframes.

4.2 Establish a secondary point of contact with US-CERT, and update OCIO-14 accordingly.

4.3 Follow existing policies and procedures to ensure applicable security incidents are correctly and timely reported to law enforcement.

Management Response

OCIO concurred with the recommendations.

REPORTING METRIC NO. 5—Risk Management

FISMA FY 2013 Audit Results

The Department did not fully comply with this reporting metric.

Issue 5a. Risk Management Program Is Not Fully Implemented (Repeat Finding)

OCIO still has not fully implemented NIST SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems," February 2010. This revision changed the traditional focus of certification and accreditation to a more dynamic approach to managing information security risks. This new approach provides agencies with the capability to more effectively manage information system-related security risks in diverse environments of complex and sophisticated cyber threats, ever-increasing system vulnerabilities, and rapidly changing missions. Since 2010, 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. As a result, personnel did not have current Department 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.

Issue 5b. System Authorization Process Needs Improvement (Modified Repeat Finding)

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

As of March 2013, the Department reported a total of 206 systems in its inventory. The inventory consisted of 46 Departmental systems, 159 contractor-owned systems, and 1 system

with no identified affiliation.[17] For these 206 systems, 126 systems (61 percent) were found to 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 206 systems we identified that:

- 31 (15 percent) were operating on expired security authorizations,
- 71 (34 percent) were operating on expired self-assessment dates, and
- 78 (38 percent) were operating on expired contingency plans that were not timely tested.

For a more in-depth review of the system authorization process for the Department's risk management program, we judgmentally selected 16 of the 206 systems. Of the 16 systems we reviewed, we found 2 systems that did not have a consistent Federal Information Processing Standards Publication 199 system categorization level for its system security plan and FISMA FY 2013 inventory listing. Specifically, the FSA RATIONAL and Literacy Information and Communications System systems were listed as moderate-impact systems in the FY 2013 inventory, while their respective system security plans were listed as a low-impact systems.

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 was not effectively and consistently certifying and accrediting 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 security weaknesses are corrected or mitigated.

Final Reports Issued From FY 2011 Through 2012 Relating to Incident Risk Management

We identified similar risk management issues in our FY 2012 FISMA audit. Specifically, OCIO did not timely implement a risk management program consistent with NIST SP 800-37, Revision 1.[18] Further, the OIG found deficiencies in system security plans, authorization to operate documents, memoranda of understanding, security assessment reports, and expired system authorizations (formerly called certification and accreditation). In addition to the FY 2012 FISMA audit, risk management issues were reported in audits dating back to FY 2011.[19]

[17] The one system was identified as neither a Departmental system nor a contractor-owned system.
[18] "Guide for Applying the Risk Management Framework for Federal Information Systems," February 2010.
[19] See report ED-OIG/A11L0001, A11M0002, and A11M0003.

Recommendation

We are making no new recommendations because corrective actions to address three recommendations contained in the FY 2011 FISMA report are still outstanding.

Management Response

OCIO concurred with the findings.

REPORTING METRIC NO. 6—Security Training (Repeat Finding)

FISMA FY 2013 Audit Results

The Department did not fully comply with this reporting metric. The OCIO continued to not follow OMB policy and NIST guidelines and allowed new users access to the Department's network before they received IT security awareness and training. OMB policy and NIST guidelines require that new users receive IT security awareness training before they are allowed access to the systems.[20] We found that the OCIO IT security awareness and training program policies were still not fully updated to meet current FISMA guidance from OMB, Office of Personnel Management, and NIST in regards to new users. The outdated policies allowed new users to access the network first and then complete the training within 10 working days of employment or initiation of a contract.

In response to our FY 2012 FISMA recommendation, the OCIO developed a "New Employee Cyber Security and Privacy Orientation" course that was provided as part of the Department's Corporate Onboarding Process, EDStart on-line, and was posted on the Department's Website. However, during our FY 2013 FISMA audit fieldwork, OCIO officials informed us that the "New Employee Cyber Security and Privacy Orientation" course proved to be ineffective and they were no longer requiring new users to complete the course. Instead, OCIO planned to develop an IT security awareness training handout that will be provided to new employees during the onboarding process.

Federal agencies and organizations cannot protect the integrity, confidentiality, and availability of information in today's highly networked systems environment without ensuring that all persons involved understand their roles and responsibilities and are adequately trained to perform them. All users of the Department's automated information systems must be able to apply the concepts of the IT security policies and be able to recognize and take appropriate steps to avert IT security situations. For the Department's programs to achieve their objectives, each user of the Department's IT resources needs to assume responsibility for IT security.

[20] OMB Circular A-130, Appendix III, November 28, 2000; Federal Register 06-14-2004, 5 C.F.R. § 930.301; and NIST SP 800-53, Revision 3, "Security and Privacy Controls for Federal Information Systems and Organizations," August 2009.

Final Reports Issued From FY 2010 Through 2012 Relating to Security Training

We also identified the current security training condition in our FY 2011 and 2012 FISMA audits.

Recommendation

We are making no new recommendations because corrective actions to address two recommendations contained in the FY 2011 FISMA report are still outstanding.

Management Response

OCIO concurred with the finding.

REPORTING METRIC NO. 7—Plan of Action and Milestones

FISMA FY 2013 Audit Results

The Department generally complied with this reporting metric. We found that the Department established and maintained a program to oversee systems operated on its behalf by contractors or other entities. This program does the following:

- has documented policies and procedures for managing IT security weaknesses discovered during security control assessments that require remediation;
- tracks, prioritizes, and remediates weaknesses;
- ensures remediation plans are effective for correcting weaknesses;
- establishes and adheres to milestone remediation dates;
- ensures resources and ownership are provided for correcting weaknesses;
- has POA&Ms that 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);
- identifies costs associated with remediating weaknesses; and
- requires program officials to report progress on remediation to Chief Information Officer on a regular basis, at least quarterly, and Chief Information Officer centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly.

Although we found that the Department has policies and procedures for managing and remediating IT security weaknesses, dates to implement corrective actions are often extended beyond the original milestone remediation date. Extending the milestone dates results in remediation delays and repeat or modified repeat findings. Further, we found that remediation plans typically address system-specific issues instead of identifying systemic issues enterprise-wide. As a result, modified repeat findings are reported.

REPORTING METRIC NO. 8—Remote Access Management

FISMA FY 2013 Audit Results

The Department did not fully comply with this reporting metric.

Issue 8a. Data Transmission and Storage Restriction Can Be Bypassed

By allowing users to use cloud storage and file sharing services (such as Google Drive), the Department enabled employees to bypass restrictions for transmitting data and storing agency information unencrypted using 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-06-16, "Protection of Sensitive Agency Information," states that when personally identifiable information 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 provide any restrictions that regulate the transmission and storage of data using public cloud solutions. We also noted that the terms of service for one provider allowed the provider to use, store, reproduce, create derivative works, publicly display and distribute the content uploaded to their 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 personally identifiable information about employees, students, and other Department customers.

Issue 8b. Remote Access Policy Needs Improvement (Repeat Finding)

Although the Department established an overall telework policy, the OCIO did not have a detailed or comprehensive telework policy reflecting the security requirements needed to establish a secure teleworking and remote access environment. In response to the FY 2011 FISMA report, OCIO developed a Telework Security Guidance document, which was originally scheduled to be disseminated by May 2012. However, OCIO officials informed us that the remote access and telework security policy was still in draft format and had not yet been finalized. Without a final Telework Security Guidance document, administrators cannot consistently enforce telework requirements and mandates. Current documentation does not adequately explain to administrators and teleworkers what they are permitted to do and what procedures they must follow when teleworking. This may increase the risk that unauthorized access to Department systems will occur.

NIST SP 800-46, Revision 1, "Guide to Enterprise Telework and Remote Access Security," states that a telework security policy should define which forms of remote access the organization permits, which types of telework devices are permitted to use each form of remote access, the type of access each type of teleworker is granted, and how user account provisioning should be handled. The policy should also cover how the organization's remote access servers are administered and updated, and how the organization plans to periodically perform assessments to confirm that the remote access policies, processes, and procedures are being properly followed.

In September 2013, OCIO provided a draft version of a telework and remote access security guidance that had not been formally reviewed or approved. OCIO officials stated that the guidance is expected to be finalized at the end of the fiscal year.

Issue 8c. Mobile Devices Testing Documentation Process Needs Improvement

OCIO was not able to furnish the test plans for mobile devices to show they were tested before being used. Specifically, we were unable to validate that testing was performed and documented for mobile devices that had already been authorized for use as a part of the "bring your own device" initiative and government furnished equipment (GFE) deployed to Federal employees. NIST SP 800-124, "Guidelines on Cell Phone and PDA Security," [21] states organizations should ensure that handheld devices are deployed, configured, and managed to meet the organizations' security requirements and objectives. Organizations should ensure an ongoing process of maintaining the security of handheld devices throughout their lifecycle. Although the OIG requested documentation showing that test plans were prepared and testing was performed for mobile devices, we did not receive any supporting information. All new solutions should be validated before they are placed in production. The Department should validate the impact new solutions may have on security to the current infrastructure. Failure to properly test new solutions could expose the network to unforeseen security issues and weaken the current security posture.

Although the Department was unable to provide test plans for the mobile device management currently in place, OCIO officials did provide test plans for the mobile device management solution the Department was planning to migrate to in the near future.

Issue 8d. Mobile Devices Not Configured To Display Government Resource Login Banner

The Department's GFE mobile devices were not configured to display a login banner to alert users they are accessing Government resources.[22] NIST SP 800-53, Revision 3, AC-8 System Use Notification, require agencies' information systems to display an approved system use notification message or banner before granting access to the system. The notification should provide privacy and security notices consistent with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Specifically, it should state that users are accessing a U.S. Government information system; system usage may be monitored, recorded, and subject to audit; unauthorized use of the system is prohibited and subject to criminal and civil penalties; and use of the system indicates consent to monitoring and recording.

The Department is not consistently and effectively following NIST guidelines for configuring GFE mobile devices to display a notification message or banner before granting access to Department systems. Specifically, OCIO officials informed us that users with issued GFE mobile devices were currently not being alerted that they were accessing a Government network via a login banner. However, OCIO officials informed us that a Department Risk Analysis Form

[21] NIST SP 800-124, "Guidelines on Cell Phone and PDA Security," October 2008, was superseded by NIST SP 800-124, Revision 1, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," June 2013.
[22] Mobile devices include Blackberry communications devices, Apple iPhone and iPad devices, Android devices, and Dell Streak devices.

was being developed to document the decision not to implement login banners for its mobile devices.

Login banners are particularly important for alerting government employees that they do not have a reasonable expectation of privacy in Government computers. Warning messages that appear before a user logs in can deter unauthorized use, increase IT security awareness, and provide a legal basis for prosecuting unauthorized access. It is especially necessary to alert users of the Bring Your Own Devices initiative that they are accessing Government resources and must comply with Government guidelines and that they may be subject to monitoring and recording of their activity while connecting to Government resources.

Issue 8e. Mobile Device Management Policies and Procedures Needs Improvement

OCIO did not have current standard operating procedures to support the Department's current mobile device management solution.[23] OCIO stated that the Department's current mobile device management solution was covered under the "IS Messaging, Department of Education Email Administration" guidance. However, our review of the document showed that the Department's mobile device management solution was not included in the document. Further, we found that the information contained in the document addressed systems and infrastructure that were obsolete and that did not reflect the current infrastructure in place. Failure to have documentation that is indicative of the current infrastructure is detrimental in troubleshooting and protecting the network from a security breach or other unforeseen issues.

Issue 8f. Two-Factor Authentication Not Fully Implemented (Modified Repeat Finding)

The OCIO still has not fully implemented and enforced the use of two-factor authentication when accessing the Department's systems to comply with DHS and OMB guidance[24] requiring two-factor authentication. The Department has been in the process of implementing and enforcing the use of two-factor authentication for all Federal employees, contractors, and other authorized users since 2010. According to FSA officials, the Department was in Phase 4 of the implementation process, which included two-factor authentication tokens being distributed to financial partners to include guaranty agencies, Title IV Additional Servicers, Third-Party Servicers, and not-for-profits. In addition, FSA reported that as of May 2013, 74,656 two-factor authentication tokens were issued, of which 883 were issued to guaranty agency users. Although the users have been issued two-factor authentication tokens, we found that only 76 percent of the tokens distributed to postsecondary schools and financial partners were registered for use. In addition, only 48 percent and 60 percent of tokens distributed to Departmental employees and FSA contractors, respectively, were registered. In addition, two-factor authentication was not implemented for accessing Web mail. OCIO informed us that the Department was in the process of implementing a new virtual private network solution that will require authorized users, both Federal employees and contractors, to dual-authenticate before being able to access Web mail through the virtual private network portal.

[23] Centralized mobile device management technologies are a growing solution for controlling the use of both organization-issued and personally-owned mobile devices by enterprise users.

[24] 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 M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information."

Allowing users to sign on without two-factor authentication could expose data and user accounts, and it could allow an intruder to access the network to conduct cyber-attacks. During the audit, the OIG became aware of mailboxes that were compromised and credentials that were used to access Web mail. As a result of this compromise, phishing emails were generated and sent to internal and external recipients. In addition, we identified an externally accessible system that processes personally identifiable information that did not require two-factor authentication which was at risk for data exposure.

Issue 8g. Data Storage on External Devices Process Needs Improvement (Repeat Finding)

According to OCIO-15, "Handbook for Sensitive But Unclassified Information," users are not allowed to save to external devices, such as flash drives or compact discs, without using Department-approved encryption, but there is no technical or automated solution to enforce this restriction. OMB Memorandum 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 flash drives, unless the information is properly encrypted. Currently, there is no technical solution deployed that allows OCIO to mandate the use of endpoint encryption when saving to an external device. OCIO stated they were aware of this vulnerability and are currently working on a pilot program to resolve the issue. Without the use of encryption for external devices, the Department runs the risk of data leakage by exposing information to unauthorized sources.

Issue 8h. Security Requirements Were Not Being Enforced on GFE

The Department did not consistently enforce security requirements for GFE laptops before users remotely accessed the Department's network. NIST SP 800-46, Revision 1, "Guide to Enterprise Telework and Remote Access Security," states that organizations should be responsible for securing their own telework client devices. According to OCIO and Dell officials, for those employees with GFE laptops that did not connect to the network on a regular basis, it was the responsibility of the user to ensure that their laptops contained all the necessary security protections (such as patching, antivirus updates, etc.). Consequently, the GFE users had the ability to connect to the network without the devices security posture being validated by the Department. Allowing users to connect via insecure GFE computers could expose the network to vulnerabilities and malware affecting those systems used to remotely connect.

Issue 8i. Policy on Removable Storage Devices Needs Improvement

The Department does not currently 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.

Issue 8j. Configuration of Non-Government Furnished Equipment Process Needs Improvement (Repeat Finding)

The Department is not consistently enforcing the telework requirement for the configuration of non-GFE to ensure the security for those devices before users remotely access the Department's network. NIST SP 800-53, Revision 3, IA-3, "Device Identification and Authentication," requires agencies' information systems to authenticate devices before establishing remote and wireless network connections by using cryptographically based, bidirectional authentication between devices. OCIO and Dell officials have policies in place that require the Department to secure non-GFE devices before the devices are authorized to connect to the network remotely. Securing non-GFE devices includes making sure antivirus software is active, personal firewalls are active, and appropriate system patching has occurred. However, no procedures are in place to validate that these required actions have occurred, which allows users to transfer data without any security restrictions. The transmission of data between an unsecured non-GFE device and a network resource could expose the internal network to malware or other vulnerabilities. It is imperative to validate the security posture of all devices connecting to network resources to ensure devices do not expose the network to any unforeseen vulnerability.

Issue 8k. Trusted Internet Connection Process Needs Improvement

The Department did not develop adequate corrective action plans for addressing the DHS Cybersecurity Capability Validation (CCV) report findings. The DHS Federal Network Security Branch's Cybersecurity Assurance Program annually assesses the state of operational readiness and cybersecurity risk of unclassified networks and systems across the Federal Civilian Executive Branch. The Cybersecurity Assurance Program is responsible for coordinating annual CCVs using an objective, repeatable and consistent validation assessment method to measure the degree of adherence to the TIC Initiative and OMB published Federal cybersecurity requirements.

Based on our review of the 2012 CCV report, we found that a total of 15 findings were reported. OCIO officials stated that OVMS was used to track and prioritize any findings from the CCV reports. To test whether the Department was adequately tracking the CCV report findings, we pulled data from OVMS to analyze. Based on our analysis conducted in June 2013, the Department did enter the 2012 CCV report findings into OVMS; however, the Department did not develop adequate corrective action plans for remediating all of the findings. Specifically, a total of 14 of the 15 findings uploaded in OVMS from the 2012 CCV report did not contain an estimated completion date or remediation date. In addition, the findings did not contain a mitigation strategy or a point of contact for remediating the findings. In September 2013, the OCIO provided documentation showing that the Department was tracking the estimated completion dates and mitigation strategies for the TIC issues identified in the CCV report outside of OVMS.

The Department's POA&M Standard Operating Procedures states that all findings or security weaknesses (including those identified as a significant deficiency or material weakness or as part of a security deviation request) must be included in and tracked on the POA&M. Additionally,

weaknesses to be recorded and tracked throughout the POA&M can be identified by auditors/reviewers or security assessments.

The TIC is a high-priority initiative mandated by OMB and DHS to optimize and standardize the security of the Federal government's network connections. The TIC implementation is designed to improve agencies' security posture and incident response capabilities. By not developing adequate corrective action plans to address findings/weaknesses from the CCV reports, the Department runs the risk of not correcting the TIC capability gaps identified by DHS in an effective and timely manner.

In addition, without the proper review and maintenance of POA&M activities, Department management may not be aware of the security control weaknesses and the severity of weaknesses within various systems and the potential or actual impact of such weaknesses on other systems. Additionally, without adequate monitoring, management may be unaware of the status of corrective actions and may not be able to assess and prioritize the resources needed to implement corrective actions.

Final Reports Issued From FY 2010 Through 2012 Relating to Remote Access Management

We identified remote access management issues in our FY 2012 FISMA audit. Specifically, OCIO did not have comprehensive or complete remote access and telework security policies and procedures and did not enforce the use of two-factor identification. In addition to the FY 2011 FISMA audit, remote access management issues were reported in audits dating back to FY 2010.[25]

Recommendations

We recommend that OCIO:

8.1 Update OCIO-15, "Handbook for Sensitive But Unclassified Information" to include restrictions for data transmissions and storage using public cloud solutions.

8.2 Establish and implement a login banner for all GFE mobile devices.

8.3 Test new mobile devices before placing them in a production environment.

8.4 Perform and document the current mobile device management solution if OCIO plans to continue using this solution in conjunction with the new Sonic Firewall solution.

8.5 Add the mobile device management solution and other similar management solutions to an updated version of the "IS Messaging Department of Education Email Administration" document.

8.6 Update the "IS Messaging Department of Education Email Administration, Version 1.1" document to reflect the current infrastructure.

[25] See reports ED-OIG/A11L0001, L21K0002, and A11L0003.

8.7 Fully implement two-factor authentication on all remote connections.

8.8 Update OCIO-01, "Handbook for "Information Assurance Security Policy," Section 4.8, Mobile Electronic Devices, and ensure all removable storage devices are scanned by the Department's antivirus software upon being connected to GFE laptops.

8.9 Provide security validation and support to remote users accessing network resources via GFE computers that do not regularly connect to the network.

For the modified and repeat findings, we are not making any additional recommendations. Corrective actions to address three recommendations contained in the FY 2011 and FY 2012 FISMA report are still outstanding**.**

Management Response

OCIO partially concurred with the Recommendations 8.2 and 8.3 and concurred with all other recommendations for this reporting metric.

For Recommendation 8.2, OCIO stated that it intends to provide a login banner for authorizing remote access solutions via virtual private network technologies including virtual private network technologies available for mobile devices (that is, not the same as mobile device management). However, OCIO does not intend to provide a login banner for accessing mobile device management solutions to reach personal information management systems (such as, email, calendar, contacts, and tasks). OCIO will develop a Risk Acceptance Form for mobile device managment solutions related to the login banner and dual-factor authentication on mobile devices by December 15, 2013.

For Recommendation 8.3, OCIO stated that it tests all GFE devices that are introduced to the EDUCATE environment. OCIO will institute a mobile device (smart phone, tablet, etc.) testing template and require the template to be completed and provided as part of the Security Risk Analysis supporting documentation that must be provided and approved before being allowed through the Enterprise Architecture Review Board implementation stage gate. OCIO is in the process of complying with the OIG recommendation, and intends to finalize the template to address this recommendation by January 30, 2014.

OIG Response

OIG agrees with OCIO's proposed approach for corrective actions and remediation dates.

REPORTING METRIC NO. 9—Contingency Planning (Modified Repeat Finding)

FISMA FY 2013 Audit Results

The Department did not fully comply with this reporting metric. OCIO and FSA did not consistently document the IT recovery procedures for their systems in accordance with federal guidelines and departmental policies. Specifically, 13 of 16 (81 percent) system contingency plans we reviewed did not include all the required contingency planning elements identified in

NIST and Departmental guidance.[26] For example, we found that contingency plans did not (1) document defined training requirements, (2) identify an alternate storage site for system backups, (3) provide a description of backup procedures to include the frequency of backups, or (4) identify the alternate telecommunication services. This occurred because OCIO did not ensure contingency plans included all required elements in accordance with NIST requirements 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. Without proper contingency planning to ensure that services provided by systems are able to operate effectively without excessive interruption, systems may not be able to recover quickly following a service disruption or disaster.

Final Reports Issued From FY 2010 Through 2012 Relating to Contingency Planning

We also identified contingency planning issues in the FY 2012 FISMA audit. Specifically, OCIO relied on contingency plans that were missing required elements identified in NIST and Department guidance.[27] In addition to the FY 2011 FISMA audit, contingency planning issues were reported in audits dating back to FY 2010.[28]

Recommendations

We recommend OCIO and FSA:

9.1 Review and update information system contingency plans for the 13 systems that have elements missing (list provided to OCIO) to ensure that all the contingency planning elements are included as required by NIST guidance.

9.2 Review all the Departmental systems' contingency plans to ensure that all required information is included in each plan as required by NIST guidance.

For the modified and repeat findings, we are not making any additional recommendations. Corrective actions to address four recommendations contained in the FY 2011 and FY 2012 FISMA report are still outstanding.

Management Response

OCIO concurred with the recommendations.

[26] 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," July 12, 2005.
[27] 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," July 12, 2005.
[28] See reports ED-OIG/A11L0003, A11L0001, and A11J0006.

REPORTING METRIC NO. 10—Contractor Systems

FISMA FY 2013 Audit Results

The Department generally complied with this reporting metric. As of March 2013, the Department's system inventory identified 159 contractor-operated systems. According to OCIO, whether the systems are contractor-operated or agency-operated, all Departmental systems reported in the system inventory are required to meet the security requirements set forth by FISMA, OMB, and NIST. We found that the Department has established and maintained a program to oversee systems operated on its behalf by contractors or other entities. This oversight program included the following:

- policies and procedures that identified information security oversight of systems operated on the agency's behalf by contractors or other entities to include contract monitoring;
- sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and organizational guidelines;
- an inventory that identifies systems operated on the agency's behalf by contractors or other entities;
- an inventory that identifies interfaces between these systems operated on the agency's behalf by contractors and agency-operated systems;
- appropriate required agreements (for example, memorandums of understanding, interconnection security agreements, or contracts) for interfaces between these systems and those that it owns and operates; and
- an inventory of contractor systems that was updated at least annually.

The Department is still in the process of implementing the continuous monitoring element to the security authorization process as the Department is transitioning to a continuous security authorization (CSA) process. This would allow for system reviews on an annual basis and provide a near real-time depiction of systems' security postures. We were informed that the systems are transitioned into the CSA program as systems come up for recertification and that new systems are automatically enrolled into the CSA program. However, if a systems' contractual requirement does not allow for transition to the new CSA process, it remains in the system authorization (3-year cycle) program. FSA officials informed us that enrollment in the CSA program depends on some of their systems' current contractual requirements that may not allow the transition to the CSA process. In those situations, the systems would remain in the system authorization process until contract revisions can be made that would allow the systems to transition to the CSA program.

Although the Department has policies and procedures for information security oversight of contractor operated systems, they are not always being followed. Prior audit reports, as well as deficiencies identified in Findings 2 through 9, show that these systems do not always comply with Federal regulations and guidance.

REPORTING METRIC NO. 11 – Security Capital Planning

FISMA FY 2013 Audit Results

The Department complied with this reporting metric. Specifically, the Department has established a security capital planning and investment program by effectively planning, tracking, and reporting funds being spent on information security to ensure that resources are available to maintain the Department's security posture. We found that the Department's security capital planning and investment program for information security included the following attributes:

- documented policies and procedures to address information security in the capital planning and investment control process,
- information security requirements as part of the capital planning and investment process;
- a discrete line item for information security in organizational programming and documentation,
- a business case (Exhibit 300 and Exhibit 53) to record the information security resources required, and
- information security resources that are available for expenditure as planned.

OTHER MATTERS

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

OCIO's Progress on Implementing Recommendations

As a part our FY 2012 FISMA audit work, DHS requested that we indicate the Department's progress in implementing recommendations from prior OIG audit reports to correct weaknesses identified in several IT areas. These areas included configuration management, identity and access management, incident response and reporting, risk management, and security training. As part of our audit fieldwork in FY 2012, we identified seven reports that were issued during FYs 2009 through 2011 to determine whether the Department had taken action in implementing the recommendations in the reports.[29] We used the Audit Accountability and Resolution Tracking System to identify and review the corrective action plans for implementing each of the recommendations.[30] For recommendations that were reported as completed, we reviewed the supporting documentation to validate that the OCIO had taken corrective actions with respect to each recommendation. We found the Department had implemented 93 of the 129 recommendations contained in the 7 reports.

At the beginning of the FY 2013 FISMA audit, we identified 36 recommendations that remained outstanding as of the close of the FY 2012 FISMA audit. To follow up on the progress made by OCIO in addressing the remaining outstanding recommendations, we followed the same procedures used to verify the completion of corrective action plans during our FY 2013 FISMA audit. During FY 2013, we found that the Department made significant progress by implementing 29 of the 36 outstanding recommendations, with the remaining 7 recommendations scheduled to be completed within the next 2 fiscal years.

Validation Testing of OVMS Information

OVMS is designated as the system of record for Departmental systems documentation. During the FY 2011 FISMA audit, when asked for system documentation, FSA officials requested that

[29] "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 Department Utility for Communications, Applications, and Technology Environment (EDUCATE)," September 2011 (ED-OIG/A11L0001); "Incident Response and Reporting Procedures," June 2011 (Investigative Program Advisory Report ED-OIG/L21L0001); "Weaknesses in the Process for Handling Compromised Privileged Accounts," September 2010 (Investigative Program Advisory Report ED-OIG/L21K0002); "Security Controls for Data Protection over the Virtual Data Center" September 2010 (ED-OIG/A11J0006); "Security over Certification and Accreditation for Information Systems," October 2009 (ED-OIG/A11J0001); and "Incident Handling and Privacy Act Controls over External Web Sites," June 2009 (EDOIG/A11I0006).

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

we extract the information from OVMS. Although we used OVMS to extract the system information, during the reporting process, we learned that some of the documentation obtained was not the current version for that system. During the FY 2012 FISMA audit, to ensure that we received the most current system documentation version, we requested that FSA officials provide the documentation directly, rather than having us extract it from OVMS. However, FSA officials stated that OVMS contained the most current system documentation and requested that we continue to use OVMS for the system documentation.

To validate whether OVMS contained the most current information regarding systems documentation, at the beginning of the FY 2013 FISMA audit, we agreed to perform validation testing of the system documentation within OVMS.

As a part of our FY 2013 FISMA planning work, we performed follow-up validation testing of OVMS using the judgmental sample of 16 systems that were selected during the FY 2012 FISMA audit. Our objective was to determine whether OVMS maintained the most current documentation for the 16 systems to include authorizations to operate, systems security plans, security assessment reports, and contingency plans. Our testing found the following:

- 1 of 16 systems was operating on expired security authorization dates,
- 4 of 16 systems were operating on an expired security assessment report or documentation could not be located,
- 11 of 16 systems were operating on expired contingency plan test dates or documentation could not be located, and
- 13 of 16 systems were operating on expired configuration management plans or documentation could not be located.

The Department needs to ensure that system owners are maintaining the most recent version of system documentation in OVMS so that current information is readily available to decision makers and auditors.

FSA VDC Disaster Recovery Exercise

As a part of FY 2013 FISMA work, we observed the FSA's execution of its disaster recovery exercise for its VDC environment, which took place at the Department's disaster recovery hot site facility in Philadelphia, Pennsylvania.[31] Per our observation, all recovery objectives were met, and the exercise was executed in accordance with the documented plans and within established timelines. The primary responsibilities of the hot site were to facilitate the restoration and reconstitution of the VDC environment.

During our observation, we found that the following objectives were accomplished during the exercise:

- the Tivoli Storage Manager environment was restored;
- the network infrastructure (router, switches, firewalls, and Application Control Engine load balancer) was restored;

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

- two (b) (7)(E) environments were restored;
- 42 utility and application servers were restored;
- 2 (b) (7)(E), 13 (b) (7)(E), 2 (b) (7)(E), and 67 (b) (7)(E) servers were restored;
- 47 databases were restored;
- 290 tapes were shipped to the recovery facility to support Tivoli Storage Manager restoration activities;
- 5,485 tapes were shipped to the recovery facility to support mainframe restoration activities;
- 42 digital audio tapes[32] were shipped in support of the HP-UX Ignite recovery strategy;
- 34 Web sites were successfully restored during the testing activities; and
- 48 applications were successfully restored.

All Tier 1, 2, and 3 applications were restored and tested successfully. [33] In addition to the exercise objectives, secondary goals were also accomplished. For example, external partners were able to successfully access FSA applications.

FSA Guaranty Agencies and Private Collection Agencies Security Review Reports

As part of our FY 2013 FISMA review, we learned that FSA performed 54 high-level security assessments (31 for guarantee agencies and 23 for private collection agencies) from FY 2009 through FY 2012. FSA reviewed certain operational controls related to the agencies' data security environments, with a specific focus on the protection of personally identifiable information. Guaranty agencies and private collection agencies manage sensitive Departmental information that needs to meet specific Federal guidelines relating to the security of that data. Our review of the 54 security assessment reports concluded that assessment objectives were well defined, and the results provided a significant amount of information relating to the specific agency's security controls. Security control issues identified during agency reviews were well-documented within the report along with recommendations and corrective actions to be taken.

OCIO Guidance Document Not Correctly Updated

During our audit fieldwork, we found an instance where OCIO updated an official guidance document without revising the version number or date. In response to our FY 2011 FISMA report, OCIO provided us with an updated version of the "IT Security Training Awareness Program Guidance," dated June 2012. This document included the process for all newly hired employees to complete the IT security awareness training through EDStart—the Department's new user onboarding and IT security awareness and training course—before being granted access to the Department's network or any Departmental information systems. When we requested the same guidance for the FY 2013 FISMA audit (provided in March 2013), we found that the language about the new user onboarding and IT security awareness and training course was removed. Further, we could not identify any evidence showing version control, newly

[32] Digital audio tapes are a type of magnetic tape that use a scheme called helical scan to record data. A digital audio tape cartridge is slightly larger than a credit card in width and height and contains a magnetic tape that can hold from 2 to 24 gigabytes of data.

[33] Tier 1, 2, and 3 applications are the applications that were deemed in scope for the April 2013 Disaster Recovery Exercise. The tier levels were determined as part of an earlier system authorization activity, based on the system criticality and sensitivity levels (determined by confidentiality, integrity, and availability).

issued date, or revision approval for the document. The IT Security Training Awareness Program Guidance document OCIO provided us in March 2013 was the same version number and date as the IT Security Training Awareness Program Guidance document provided to us in June 2012. Furthermore, there was no indication in the Document Change History that the guidance was updated.

By not correctly updating and tracking revisions made to official policy and guidance documents, users are not aware of changes and, therefore, could follow outdated and incorrect policies and procedures. The Department runs the risk of employees performing their job functions incorrectly and making errors. We suggest the Department develop, or strengthen existing procedures, to ensure official policy and guidance documents are updated and tracked correctly so users are aware of any changes to the documents.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine whether the Department and FSA's overall information technology 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. Specifically, we 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.

This report constitutes the OIG's independent evaluation of the Department's IT security program and practices, as required by the FISMA. The OIG's review is based on metrics and questions DHS provided for the FY 2013 FISMA review, which are designed to annually assess the status of the Department's security posture. For FY 2013 FISMA reporting, each IG was required to evaluate its respective agency on the following 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
- Security Capital Planning

As of March 2013, the Department reported an inventory of 206 IT systems. For FY 2013 FISMA reporting, we judgmentally selected, based on several factors, 16 of the Department's systems. Because the Department is currently transitioning its systems from the system authorization program to the CSA program (as part of the Risk Management Framework approach required in NIST 800-37, Revision 1, "Guide for Applying The Risk Management Framework to Federal Information Systems"), we selected 8 systems that were enrolled in the CSA program. Also, our systems selection included systems owned by both contractors and the Department. Each year, to ensure that our judgmental sample reflects an accurate representation of the Department's systems, we attempted to select systems that were not reviewed during our last two FISMA audits. For the judgmentally selected systems, our review focused on security control aspects relating to risk management, configuration management, and contingency planning.

The table below lists the systems selected, the system's Principal Office, and the Federal Information Processing Standards Publication 199 potential impact level. While we reviewed whether specific security controls were implemented at a system-level, we evaluated enterprise-

wide IT systems management overall. The OCIO is charged with implementing the operative principles established by legislation and regulation, establishing a management framework to improve the planning and control of IT investments, and leading change to improve the efficiency and effectiveness of Department operations. Therefore, we evaluated FISMA compliance of the OCIO's management of Department IT systems and enterprise-wide policies, procedures, and implementation.

Number	System Name	Principal Office	Level
1	Virtual Data Center	FSA	High
2	ACS Education Servicing System	FSA	Moderate
3	Common Origination and Disbursement	FSA	Moderate
4	Central Processing System	FSA	Moderate
5	Debt Management Collection System 2	FSA	Moderate
6	e-Campus Based	FSA	Moderate
7	National Student Loan Database System	FSA	Moderate
8	Operational Vulnerability Management Solution	FSA	Moderate
9	Postsecondary Educational Participants System	FSA	Moderate
10	FSA Rational	FSA	Moderate
11	Student Aid Internet Gateway	FSA	Moderate
12	ED Enterprise Architecture Tool	OCIO	Moderate
13	EDUCATE Security	OCIO	Moderate
14	Office of the General Counsel Case and Activity Management System	OGC*	Moderate
15	OIG Local Area Network	OIG	Moderate
16	Literacy Information and Communications System	OVAE*	Moderate

* Office of the General Counsel, Office of Vocational & Adult Education.

In addition to our FISMA fieldwork, we incorporated the results of the vulnerability and penetration testing performed at FSA's VDC into this year's FISMA review.

The audit covered the Department's management of IT security programs and systems for FY 2013. We conducted fieldwork from February 2013 through July 2013, primarily at Departmental offices in Washington, D.C., and contractor facilities in Philadelphia, Pennsylvania, and Plano, Texas. During our fieldwork, penetration and vulnerability testing was performed by SeNet International Corporation, on behalf of the OIG, at the VDC in Plano, Texas. Specifically, we performed the internal vulnerability assessment during March 2013 and the external scanning during April 2013. Our FY 2013 FISMA audit also included an evaluation of prior audit coverage, as well as the Department's progress in implementing recommendations and correcting IT security weaknesses resulting from reports issued during FY 2010 to the present. We held an exit conference on September 23, 2013.

To accomplish our objectives, we performed the following procedures:

- reviewed Department policies and procedures and manuals, comparing these to procedures described in the system security plans and system authorization documents;
- reviewed contractor guides and other program guidance to gain an understanding of IT security controls in place as they relate to protection of Department resources;
- interviewed Department officials, including officials with specific IT security roles related to the IT security controls areas;
- interviewed contractor personnel to gain an understanding of the system security and application of management, operational, and technical controls; and
- compared and tested management, operational, and technical controls in place based on NIST standards and Department guidance.

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 and Remote Access Management, and Risk Management areas that were used to support the findings summarized in the FY 2013 FISMA 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.

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.

Inspector General

Section Report

2013

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's Compliance with the Federal Information Security Management Act for Fiscal Year 2013," Audit Control No. ED-OIG/A11N0001, Reporting Metric No. 1, Continuous Monitoring Management, hereafter referred to as FISMA Report.

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 and plans for continuous monitoring (NIST SP 800-37 Rev 1, Appendix G).

Yes

Comments: No exceptions noted.

1.1.3 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, NIST 800-53A).

Yes

Comments: No exceptions noted.

1.1.4 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

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: FISMA Report: Reporting Metric No. 2, Configuration Management

2.1.1 Documented policies and procedures for configuration management.

No

Comments: FISMA Report: Reporting Metric No. 2, Configuration Management, Issue 2b- Patch Management Program Needs Improvement

2.1.2 Defined standard baseline configurations.

No

Comments: FISMA Report: Reporting Metric No. 2, Configuration Management, Issue 2a- Configuration Management Plans Were Not Consistently Developed (Modified Repeat Finding)

2.1.3 Assessments of compliance with baseline configurations.

Yes

Comments: No exceptions noted.

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

Section 2: Configuration Management

2.1.7 Process for timely and secure installation of software patches.

No

Comments: FISMA Report: Reporting Metric No. 2, Configuration Management, Issue 2c- Patch Management Process Needs Improvement (Modified Repeat Finding)

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)

No

Comments: FISMA Report: Reporting Metric No. 2, Configuration Management, Issue 2d- Controls for Identifying and Resolving Configuration Management Vulnerabilities Need Improvement (Modified Repeat Finding).

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.

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

See Narrative for Exception Noted.

Comments: FISMA Report: Reporting Metric No. 2, Configuration Management, Issue 2e- Access Switch Port Security Needs Improvement.

Section 3: Identity and Access Management

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

Yes

Comments: FISMA Report: Reporting Metric No. 3, Identity and Access Management

Section 3: Identity and Access Management

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

No

Comments: FISMA Report: Reporting Metric No. 3, Identity and Access Management, Issue 3a- 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: Reporting Metric No. 3, Identity and Access Management, Issue 3a- 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.

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

Comments: 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.

Section 3: Identity and Access Management

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, 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.

No

Comments: FISMA Report: Reporting Metric No. 3, Identity and Access Management, Issue 3c- Users' Account Deactivation Process Needs Improvement (Modified Repeat Finding).

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 Exception Noted.

Comments: FISMA Report: Reporting Metric No. 3, Identity and Access Management, Issue 3b- Password Authentication Process Needs Improvement.

Section 4: Incident Response and Reporting

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: FISMA Report: Reporting Metric No. 4, Incident Response and Reporting.

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

Yes

Comments: No exceptions noted.

4.1.2 Comprehensive analysis, validation and documentation of incidents.

Yes

Comments: No exceptions noted.

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

No

Comments: FISMA Report: Reporting Metric No. 4, Incident Response and Reporting, Issue 4a- Incident Response and Reporting to the United States Computer Emergency Readiness Team Needs Improvement (Modified Repeat Finding).

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

No

Comments: FISMA Report: Reporting Metric No. 4, Incident Response and Reporting, Issue 4b- 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.

Section 4: Incident Response and Reporting

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: FISMA Report: Reporting Metric No. 5, Risk Management

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: Reporting Metric No. 5, Risk Management, Issue 5a- 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.

Section 5: Risk Management

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: Reporting Metric No. 5, Risk Management, Issue 5b- System Authorization Process Needs Improvement (Modified Repeat Finding).

5.1.6 Categorizes information systems in accordance with government policies.

No

Comments: FISMA Report: Reporting Metric No. 5, Risk Management, Issue 5b- 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.

Section 5: Risk Management

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.

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.

Section 5: Risk Management

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, 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: FISMA Report: Reporting Metric No. 6, Security Training.

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

No

Comments: FISMA Report: Reporting Metric No. 6, Security Training (Repeat Finding).

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.

Section 6: Security Training

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.

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.

See Narrative for Exceptions Noted.

Comments: FISMA Report: Reporting Metric No. 6, Security Training (Repeat Finding).

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: FISMA Report: Reporting Metric No. 7, Plan of Action & Milestones (POA&M).

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.

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

7.1.2 **Tracks, prioritizes and remediates weaknesses.**

Yes

Comments:

7.1.3 **Ensures remediation plans are effective for correcting weaknesses.**

Yes

Comments:

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

Yes

Comments:

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

Yes

Comments:

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:

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:

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:

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

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: FISMA Report: Reporting Metric No. 8, Remote Access Management.

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

No

Comments: FISMA Report: Reporting Metric No. 8, Remote Access Management, Issue 8e- Mobile Device Management Policies and Procedures Need Improvement.FISMA Report: Reporting Mtetric No. 8, Remote Access Management, Issue 8i- Policy on Removable Storage Devices Need Improvement.

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

Yes

Comments: No exceptions noted.

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

No

Comments: FISMA Report: Reporting Metric No. 8, Remote Access Management, Issue 8j- Configuration of Non-Government Furnished Equipment Process Needs Improvement (Repeat Finding).

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

No

Comments: FISMA Report: Reporting Metric No. 8, Remote Access Management, Issue 8b- Remote Access Management Policy Needs Improvement (Repeat Finding).

Section 8: Remote Access Management

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: Reporting Metric No. 8, Remote Access Management, Issue 8f- Two-Factor Authentication Not Fully Implemented (Modified Repeat Finding).

8.1.6 Authentication mechanisms meet NIST Special Publication 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.

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.

Section 8: Remote Access Management

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: Reporting Metric No. 8, Remote Access Management, Issue 8a- Data Transmission and Storage Restriction Can Be Bypassed. FISMA Report: Reporting Metric No. 8, Remote Access Management, Issue 8c- Mobile Device Testing Documentation Process Needs Improvement. FISMA Report: Reporting Metric No. 8, Remote Access Management, Issue 8d- Mobile Devices Not Configured to Display Government Resource Login Banner.FISMA Report: Reporting Metric No. 8, Remote Access Management, Issue 8e- Mobile Device Management Policies and Procedures Need Improvement.FISMA Report: Reporting Metric No. 8, Remote Access Management, Issue 8g- Data Storage on External Devices Process Needs Improvement.FISMA Report: Reporting Metric No. 8, Remote Access Management, Issue 8h- Security Requirements Were Not Being Enforced on GFE.FISMA Report: Reporting Metric No. 8, Remote Access Management, Issue 8k- Trusted Internet Connection Process Needs Improvement.

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

Yes

Comments: No exceptions noted.

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: FISMA Report: Reporting Metric No. 9, Contingency Planning.

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.

Section 9: Contingency Planning

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: Reporting Metric No. 9, Contingency Planning, Issue 9a- Contingency Plans Not Complete (Modified Repeat Finding).

9.1.4 Testing of system specific contingency plans.

Yes

Comments: No exceptions noted.

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.

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.

Section 9: Contingency Planning

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: FISMA Report: Reporting Metric No. 10, Contractor Systems.

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

Yes

Comments: No exceptions noted.

Section 10: Contractor Systems

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).

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.

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

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: FISMA Report: Reporting Metric No. 11, Security Capital Planning.

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.

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: Criteria

"The Federal Information Security Management Act of 2002" (FISMA), Title III of the E-Government Act of 2002, Public Law 107–347, 116 Stat. 2899, December 17, 2002

"FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics," U.S. Department of Homeland Security, Office of Cybersecurity and Communications, Federal Network Resilience, November 20, 2012

"Network Security Checklist – CISCO Layer 2 Switch," Defense Information Systems Agency, Version 7, Release 1.9, June 26, 2009

"Homeland Security Presidential Directive/HSPD-12," August 27, 2004

Office of Management and Budget (OMB) Memorandum M-05-24, "Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors," August 5, 2005

OMB M-12-20, "FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," September 27, 2012

OMB M-10-28, "Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)," July 6, 2010

OMB M-06-16, "Protection of Sensitive Agency Information," June 23, 2006

OMB M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 22, 2007

OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," revised November 28, 2000

Federal Information Processing Standards Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004

Federal Register Vol. 69, No. 113, United States Office of Personnel Management, 5 C.F.R. § 930.301, "IS Security Awareness Training," June 14, 2004

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34 Revision 1, "Contingency Planning Guide for Federal Information Systems," May 2010

NIST SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems," February 2010

NIST SP 800-46, Revision 1, "Guide to Enterprise Telework and Remote Access Security," June 2009

NIST SP 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," August 2009

NIST SP 800-53A, Revision 1, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations," June 2010

NIST SP 800-61, Revision 2, "Computer Security Incident Handling Guide," August 2012

NIST SP 800-124, "Guidelines on Cell Phone and PDA Security," October 2008

NIST SP 800-111, "Guide to Storage Encryption Technologies for End User Devices," November 2007

OCIO -01, "Handbook for Information Assurance (IA) Policy," October 19, 2011

OCIO -10, "Handbook for Information Technology Security Contingency Planning Procedures," July 12, 2005

OCIO-11, "Handbook for Information Technology Configuration Management Planning Procedures," July 12, 2005

OCIO-14, "Handbook for Information Security Incident Response and Reporting Procedures," March 2, 2011

"Logical Access Control Guidance," Version 6.1, March 28, 2013

"IS Messaging, Department of Education Email Administration," Version 1.1, April 15, 2013

"U.S. Department of Education Plan of Actions and Milestones Guidance," Version 1.3, March 15, 2013

UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF THE CHIEF INFORMATION OFFICER

THE CHIEF INFORMATION OFFICER

MEMORANDUM

DATE: November 4, 2013

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

FROM: Danny A. Harris, Ph.D.

SUBJECT: Draft Audit Report
Audit of the U.S. Department of Education's Compliance with the Federal Information Security Management Act for Fiscal Year 2013
Control Number ED-OIG/A11N0001

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 2013, Control Number ED-OIG/A11N0001. The Department sincerely 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 partnering and the sharing of mutual goals and objectives.

The Department has garnered significant benefits from previous years' audits and expects that the recommendations presented in this current audit will further improve the information security program by strengthening the associated management, technical and operational security controls. The Office of the Chief Information Officer (OCIO) will address each finding and recommendation as stipulated in the plan provided, and as agreed upon by your office.

The following OCIO responses address each recommendation:

REPORTING METRIC NO.1-Continous Monitoring

The OIG found the Department complied with this reporting metric.

REPORTING METRIC NO.2-Configuration Management

OIG Recommendation 2.1-Ensure all Department system configuration management plans are prepared uniformly to include system configuration baselines and to document system upgrades and additions to software and hardware components when applicable.

Management Response: OCIO concurs with this recommendation. Federal Student Aid (FSA) will standardize Configuration Management Plan (CMP) data requirements to include system baseline configuration data. FSA will provide updated CMPs for the Virtual Data Center (VDC), National Student Loan Data System (NSLDS), and the Operational Vulnerability Management Solution (OVMS) as evidence of closure by July 30, 2014.

OIG Recommendation 2.2-Require Dell Services Federal Government (DSFG) to comply with the patch testing and implementation procedures documented in the OCIO-01 "Handbook for Information Assurance Security Policy".

Management Response: OCIO concurs with this recommendation. FSA will continue to work with DSFG to comply with requirements for documented patch testing and implementation procedures documented. FSA will monitor the results/progress of these audit items on a monthly basis until all corrective actions are completed. FSA will provide updated extracts from the VDC SSP and the VDC Patching SOP as evidence for closure by September 30, 2014.

OIG Recommendation 2.3-Immediately corrects or mitigates the vulnerabilities identified during the vulnerability assessment.

Management Response: OCIO concurs with this recommendation. FSA will provide a listing of OVMS entries derived from the assessment for proper remediation through the Plans of Action & Milestones (POA&M) process. The critical findings identified within the Vulnerability Report have been provided to DSFG to resolve. FSA will provide a listing of all vulnerabilities contained within the Vulnerability Report provided by the audit team with corresponding OVMS entries. The vulnerability items listed in the vulnerability report will be extracted into a listing with corresponding OVMS numbers. The vulnerabilities will be remediated through the existing POA&M process. The vulnerability listing and corresponding OVMS number will be provided as evidence to close this recommendation by January 30, 2014. OIG may monitor progress within OVMS.

OIG Recommendation 2.4-Establish reporting procedures to monitor DSFG's monthly progress to ensure identified vulnerabilities are fixed within the established timelines.

Management Response: OCIO concurs with this recommendation. The Department and FSA will improve its reporting and monitoring of the patching program by distributing monthly patching reports from Qualys, and FSA will engage DSFG to provide monthly progress and status reports of all outstanding patches.

FSA will broaden the distribution of Qualys patching reporting to include DSFG, FSA Technology Office – Security & VDC Operations, FSA Application Information System Security Officers, FSA Cyber Security, Department of Education Computer Incident Response Capability (EDCIRC), and Department of Education Security Operations Center (EDSOC). FSA will engage DSFG to produce monthly status and progress reports by July 30, 2014.

OIG Recommendation 2.5-Immediately correct or mitigate the vulnerabilities with the (b) (7)(E) (b) (7)(E) and Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) web applications identified during the vulnerability assessment.

Management Response: OCIO concurs with this recommendation. OCIO will provide a listing of OVMS entries derived from the assessment for proper remediation through the POA&M process. OCIO will provide a listing of all vulnerabilities contained within the Vulnerability Report provided by the OIG with corresponding OVMS entries. The vulnerability items listed in the vulnerability report will be extracted into a listing with corresponding OVMS numbers. The vulnerabilities will be remediated through the existing POA&M process. The vulnerability listing and corresponding OVMS number will be provided as evidence to close this recommendation by January 16, 2014.

REPORTING METRIC NO.3-Identity and Access Management

OIG Recommendation 3.1-Ensure that OCIO-01 "Handbook for Information Assurance Security Policy" is enforced to require that passwords are changed every 90 days.

Management Response: OCIO concurs with this recommendation. OCIO will ensure Active Directory is configured to automatically notify and prompt users to change their network passwords after 90 days, unless otherwise documented via a Policy Exception Form (PEF) filled out and approved by the account owner, in accordance with OCIO-01 by January 31, 2014. Additionally, OCIO Information Technology Services (ITS) division will perform quarterly audits of the network accounts to validate that passwords are being updated every 90 days starting April 30, 2014.

OIG Recommendation 3.2-Enforce Departmental procedures to disable user accounts that have not been accessed for ninety days or longer, in accordance with FISMA and applicable regulations, guidance, and standards established in National Institute of Standards and Technology (NIST) guidelines.

Management Response: OCIO concurs with this recommendation. OCIO ITS will create a SOP to effectively ensure that user accounts that are found to be inactive for 90 days are disabled by April 30, 2014. The accounts will be validated once a month as per the new SOP starting June 1, 2014.

REPORTING METRIC NO.4-Incident Response and Reporting

OIG Recommendation 4.1-Follow existing policies and procedures to ensure security incidents are reported to US-CERT within the required timeframes.

Management Response: OCIO concurs with this recommendation. OCIO, in conjunction with FSA, will review and amend the appropriate process (es) to reflect reporting criteria and provide a user communication plan to ensure that third party customers are aware of and respond to United States Computer Emergency Readiness Team (US-CERT) reportable incidents in a timely manner by February 28, 2014. Additionally, metrics will be developed or modified to show the reporting status and timelines by December 1, 2013.

OIG Recommendation 4.2-Establish a secondary point of contact (PoC) with US-CERT, and update OCIO-14 accordingly.

Management Response: OCIO concurs with this recommendation. The US-CERT watch desk has the contact information for two current Department of Education PoCs for incident reporting. OCIO Information Assurance Services (IAS) will ensure that appropriate supplemental policy instructions and a periodic review process is established ensuring the US-CERT and Department of Homeland Security has current contact information. The existing US-CERT PoCs list will be updated by December 1, 2013. Documentation and process reviews with appropriate amendments will be completed by January 1, 2014.

OIG Recommendation 4.3-Follow existing policies and procedures to ensure applicable security incidents are correctly and timely reported to law enforcement.

Management Response: OCIO concurs with this recommendation. OCIO, in conjunction with OIG Technology Crimes Division (TCD), will review, amend, or develop the appropriate process (es) to reflect reporting criteria to include the required documentation for the notifications. Initial OIG TCD meeting will take place by November 30, 2013. The policy updates will be completed by January 31, 2014.

REPORTING METRIC NO.5-Risk Management

OIG Conclusion 5a.-Risk Management Program Is Not Fully Implemented (Repeat Finding)

OIG Recommendation 5a.-Corrective actions to address this recommendation contained in the FY2011 FISMA report are still outstanding. OCIO to "Fully develop and implement a risk management program, policies, and procedures (including a continuous monitoring process) consistent with FISMA and applicable regulations and standards established by Office of Management and Budget (OMB) and NIST." See http://www2.ed.gov/about/offices/list/oig/auditreports/fy2012/a11l0003.pdf, page 10 of 79.

Management Response: OCIO concurs with this recommendation, action completed. IAS defined an enterprise-wide risk management strategy and submitted it for Chief Information Security Officer (CISO) review on September 30, 2013.

OIG Conclusion 5b.-System Authorization Process Needs Improvement (Modified Repeat Finding)

OIG Recommendation 5b.-Corrective actions to address this recommendation contained in the FY2011 FISMA report are still outstanding. OCIO to "Ensure that system authorizations are completed at least every 3 years, when there are significant changes to the systems, or when systems are transitioned to continuous system authorization (whichever occurs first)." "Update the OCIO-05 and OCIO-01 handbooks to be in compliance with OMB and NIST guidance with respect to risk management and interim Authority to Operate." See http://www2.ed.gov/about/offices/list/oig/auditreports/fy2012/a11l0003.pdf page 11 of 79.

Management Response: OCIO concurs with this recommendation. OCIO IAS division will review and update appropriate Department IAS and Security policies upon approval of the Risk Management Framework implementation plan to ensure policy updates are consistent with the Department's risk management approach, as well as OMB and NIST guidance. IAS will submit recommendations for policy revisions to the CISO for approval by March 28, 2014.

REPORTING METRIC NO. 6-Security Training

OIG Recommendation- Corrective actions to address this recommendation contained in the FY2011 FISMA report are still outstanding. OCIO to "Develop a new user IT security awareness and training course that is delivered and completed prior to individuals being allowed to access the EDUCATE network or any Department information systems. See http://www2.ed.gov/about/offices/list/oig/auditreports/fy2012/a11l0003.pdf, page 18 of 79.

Management Response: OCIO concurs with this recommendation. OCIO will review the Department's onboarding Security Training process, work with Personnel and OCIO/Information Technology Services (ITS) on updating this process to ensure all new employees who received security awareness training submit an onboarding form to OCIO/ITS providing evidence of the training completion prior to be allowed access to the network. These revisions will be submitted to IAS management for review by April 30, 2014.

REPORTING METRIC NO. 7-Plan of Action and Milestones

The OIG found the Department complied with this reporting metric.

REPORTING METRIC NO. 8-Remote Access Management

OIG Recommendation 8.1-Update OCIO-01, "Handbook for Information Assurance Security Policy" to include restrictions for data transmissions and storage using public cloud solutions.

Management Response: OCIO concurs with this recommendation. OCIO will update current OCIO-01 policy document to include restrictions for data transmissions and storage using public cloud solutions. These revisions will be submitted to IAS management for review by August 31, 2014.

OIG Recommendation 8.2-Establish and implement a login banner for all Government Furnished Equipment (GFE) mobile devices.

Management Response: OCIO partially-concurs with this recommendation. OCIO does intend to provide a login banner for authorizing remote access solutions via virtual private network (VPN) technologies including VPN technologies available for mobile devices (e.g., not the same as MDM). However, OCIO does not intend to provide a login banner for accessing mobile device management (MDM) solutions to reach personal information management systems (e.g., email, calendar, contacts, and tasks). A Risk Acceptance Form will be developed for MDM solutions related to login banner and dual-factor authentication on mobile devices by December 15, 2013.

OIG Recommendation 8.3-Test new mobile devices before placing them in a production environment.

Management Response: OCIO partially-concurs with this recommendation. OCIO does test all GFE devices that are introduced to the EDUCATE environment. OCIO will institute a Mobile Device (Smart Phone, Tablet, etc.) testing template and require the template to be completed and provided as part of the Security Risk Analysis supporting documentation that must be provided and approved before being allowed through the Enterprise Architecture Review Board implementation stage gate. OCIO is in the process of complying with the OIG recommendation. Template to comply will be finalized by January 30, 2014.

OIG Recommendation 8.4-Perform and document the current mobile device management solution if OCIO plans to continue using this solution in conjunction with the new Sonic Firewall solution.

Management Response: OCIO concurs with this recommendation. Upon implementation of the pending mobile device management solution, this is the current pilot phase; OCIO will develop associated standard operating procedures to support the approved MDM solution(s). At such time, OCIO will update the "IS Messaging, Department of Education Email Administration" guidance to include the new solution, or redirect the reader to the appropriate documentation set for the deployed MDM solutions by March 28, 2014. OCIO does not intend to update the existing documentation set related to the existing MDM solution and the removal of all BlackBerry devices, which is expected to be shut down by January 31, 2014.

OIG Recommendation 8.5-Update the "IS Messaging Department of Education Email Administration" to provide a more current version that supports the current infrastructure.

Management Response: OCIO concurs with this recommendation. OCIO will update the "IS Messaging, Department of Education Email Administration" guidance to include current solutions, or redirect the reader to the appropriate documentation set for the deployed solutions by March 28, 2014.

OIG Recommendation 8.6-Add the mobile device management solution and other similar management solutions to an updated version of the "IS Messaging Department of Education Email Administration" document.

Management Response: OCIO concurs with this recommendation. OCIO will update the "IS Messaging, Department of Education Email Administration" guidance to include the new solution, or redirect the reader to the appropriate documentation set for the deployed MDM solutions by March 28, 2014.

OIG Recommendation 8.7-Configure a content management solution that helps maintain version control and the upkeep of documentation as infrastructure changes.

Management Response: OCIO concurs with this recommendation. OCIO will require the DSFG to maintain version control on all its documentation of infrastructure updates. OCIO will use the Share Point Application (EDUCATE ISSO Site) to maintain the most recent copies of System Documentation in support of the EDUCATE Systems. This will become a mandatory requirement starting April 30, 2014.

OIG Recommendation 8.8-Fully implements dual-authentication on all remote connections.

OCIO suggests changing this recommendation to: Fully implements two-factor authentication on all remote connections. .

Management Response: OCIO concurs with this recommendation. OCIO is developing solutions that will implement dual authentication on remote access solutions. OCIO intends to retire the single-based authentication for (b) (7)(E) services (i.e., (b) (7)(E)) by (b) (7)(E). OCIO does intend to implement two-factor authentication for VPN services (mobile apps) on mobile devices, but OCIO does not intend to implement two-factor authentication for device-level access to mobile devices and the associated personal information management services (e.g., email, calendar, contacts and tasks). In such case, a Risk Analysis Form will be developed for MDM solutions.

Additionally, the Department and FSA will continue to field and service the existing Two-Factor Authentication tokens for its remote users. Phases 1-4 are complete (as of 8/30/2013), Phase V is scheduled to complete October 30, 2015:

- Phase I – Department of Education users

- Phase II – Federal Student Aid users
- Phase III – Postsecondary Schools and selected financial partners
- Phase IV – Financial Partners
- Phase V – Migration to soft tokens for all users

Two-Factor Authentication (TFA) has distributed 69,235 tokens to financial aid personnel at Postsecondary Schools, Guaranty Agencies, Title IV Additional Servicers, Third-Party Servicers, and not-for-profits. Guaranty Agency users account for 877 of the privileged user population. TFA tokens have been distributed to all 34 Guaranty Agencies organizations and all Guaranty Agencies users were TFA enabled as of April 12, 2013. Quarterly progress reports will be provided as evidence of progress and closure. FSA will field the soft tokens per the existing plan, Phase V – Migration to soft tokens for all users by October 30, 2015.

OIG Recommendation 8.9-Update OCIO-01, "Handbook for "Information Assurance Security Policy", Section 4.8, Mobile Electronic Devices, and ensure all removable storage devices are scanned by the Department's antivirus software upon being connected to GFE laptops.

Management Response: OCIO concurs with this recommendation. OCIO will review current OCIO-01 policy document for "Information Assurance Security Policy", Section 4.8, Mobile Electronic Devices, and ensure all removable storage devices are scanned by the Department's antivirus software upon being connected to GFE laptops. These revisions will be submitted to IAS management for review by August 31, 2014.

Additionally, OCIO IAS will direct DSFG to ensure all removable storage devices are scanned by the Department's antivirus software upon being connected to GFE laptops March 28, 2014.

OIG Recommendation 8.10-Ensure that the draft "Telework and Remote Access Security Guidance" includes requirements to perform validation procedures to ensure the security of non-GFE devices used to connect to the Department's network remotely.

Management Response: OCIO concurs with this recommendation. OCIO will review current Telework and Remote Access Security Guidance to include requirements to perform validation procedures to ensure the security of non-GFE devices used to connect to the Department's network remotely. The revisions will be submitted to IAS management for review by April 30, 2014.

OIG Recommendation 8.11-Provide security validation and support to remote users accessing network resources via GFE computers that do not regularly connect to the network.

Management Response: OCIO concurs with this recommendation. If GFE laptops have received the "remote patching solution" that was implemented prior to July 2013, the solution should correct this issue. OCIO will periodically evaluate the inventory of GFE laptops that did not receive the "remote patching solution" and escalate with the associated POC to coordinate bringing the device into the nearest ED location to install the "remote patching solution" to subsequently allow patches to be installed.

REPORTING METRIC NO. 9-Contingency Planning

OIG Recommendation 9.1- Review and update information system contingency plans for the 13 system that have missing elements (list provided to OCIO), and include a crosswalk if the element is addressed under an overarching contingency plan, to ensure that all contingency planning elements are included as required by NIST guidance.

Management Response: OCIO concurs with this recommendation. OCIO will review the contingency plans for the five Department systems identified and issue findings against the respective systems for remediation by February 28, 2014.

FSA will review and update information system contingency plans for the 8 remaining FSA systems identified as having missing elements (list provided to OCIO/OIG), and include a cross-walk if the element is addressed under an overarching contingency plan, to ensure that all contingency planning elements are included as required by NIST guidance. FSA will submit the eight identified systems contingency plans as evidence for closure by July 30, 2014.

OIG Recommendation 9.2-Review all the Departmental systems' contingency plans to ensure that all required information is included in each plan as required by NIST guidance.

Management Response: OCIO concurs with this recommendation. OCIO IAS will review the contingency plans for Departmental systems to ensure that all required information is included in each plan as required by NIST guidance and Department policy as part of the annual security assessment process by October 30, 2014.

REPORTING METRIC NO. 10-Contractor Systems

The OIG found the Department complied with this reporting metric.

REPORTING METRIC NO. 11-Security Capital Planning

The OIG found the Department complied with this reporting metric.

Thank you for the opportunity to comment on this report and for your continued support of the Department and its critical mission. If you have any questions regarding this matter, please contact me at (202) 245-6252 or Danny.Harris@ed.gov.