The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2012

FINAL AUDIT REPORT

ED-OIG/A11M0003
November 2012

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/Acronyms Used in this Report

BCP	Business Continuity Plan
BIA	Business Impact Analysis
CIO	Chief Information Officer
Department	U.S. Department of Education
DHS	Department of Homeland Security
DSFG	Dell Services Federal Government
EDCAPS	Department of Education's Central Automated Processing System
EDMASS	EDUCATE Mass Storage System
EDNIS	Education Network Infrastructure System
EDSOC	EDUCATE Security Operations Center
EDUCATE	Education Department Utility for Communications, Applications, and Technology Environment
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
FSA	Federal Student Aid
FY	Fiscal Year
GFE	Government Furnished Equipment
ISSO	Information System Security Officer
IT	Information Technology
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SP	Special Publication
VDC	Virtual Data Center

UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Information Technology Audit Division

November 7, 2012

Memorandum

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

Richard Gordon
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 2012
Control Number ED-OIG/A11M0003

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 2012. 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
Dawn Dawson, Audit Liaison, Federal Student Aid
Linda Wilbanks, PhD, Director, Information Technology Risk Management Group / Chief Information Security Officer, Federal Student Aid
Bucky Methfessel, Senior Counsel for Information & Technology, Office of General Counsel
Randy Prindle, Post Audit Group, Office of Chief Financial Officer
L'Wanda Rosemond, AARTS Administrator, OIG

TABLE OF CONTENTS

Page

EXECUTIVE SUMMARY **1**

BACKGROUND **3**

AUDIT RESULTS **6**

REPORTING METRIC NO. 1—Continuous Monitoring Management **7**

REPORTING METRIC NO. 2—Configuration Management (Repeat Finding) **8**

REPORTING METRIC NO. 3—Identity and Access Management (Repeat Finding) **9**

REPORTING METRIC NO. 4—Incident Response and Reporting **10**

REPORTING METRIC NO. 5—Risk Management **13**

REPORTING METRIC NO. 6—Security Training (Repeat Finding) **15**

REPORTING METRIC NO. 7—Plan of Action and Milestones **17**

REPORTING METRIC. NO. 8—Remote Access Management **17**

REPORTING METRIC NO. 9—Contingency Planning **22**

REPORTING METRIC NO. 10—Contractor Systems **27**

REPORTING METRIC NO. 11—Security Capital Planning **28**

OTHER MATTERS **29**

OBJECTIVE, SCOPE, AND METHODOLOGY **30**

Enclosure 1: CyberScope FISMA Reporting **33**

Enclosure 2: Criteria **53**

Enclosure 3: Management Comments **55**

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). The OIG's review is based on questions and metrics that the Department of Homeland Security (DHS) provided for the annual FISMA review designed to assess the status of the Department's security posture in fiscal year (FY) 2012. DHS prepared the Inspector General reporting metrics, or controls areas, to be assessed for FY 2012 FISMA compliance in March 2012. The 11 controls 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 FY 2012 FISMA review, DHS's framework required us to evaluate the Department's information technology processes, policies, and procedures that the Department had already implemented and documented and was monitoring. Although the Department's many planned activities may improve its security posture in the future, the planned initiatives could not be evaluated as part of the FY 2012 FISMA review, because they were not fully operational at the time. As part of FISMA, the OIG reviewed Department systems, contractors, annual self-assessments, policies, procedures, various OIG audit reports, and other Federal agency reports issued throughout the year.

Our objective was to determine whether the Department's overall information technology security program and practices comply with the E-Government Act of 2002 (Public Law 107-347) including Title III, FISMA, and Office of Management and Budget (OMB) guidance. 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 to be compliant in 3 of the 11 reporting metrics (Continuous Monitoring, Contractor Systems, and Security Capital Planning). However, we identified findings in eight of the reporting metrics. The findings in six of the reporting metrics— Configuration Management, Identity and Access Management, Risk Management, Security Training, Remote Access Management, and Contingency Planning—contained repeat findings from OIG reports issued from FY 2009 through FY 2011.[2] We answered the questions in the DHS metrics template, based on our audit work, which will be input to the CyberScope FISMA Report as shown in Enclosure 1.

[1] For purposes of this audit, enterprise-level security controls are controls that are expected to be implemented.
[2] Repeat findings are current report findings with the same or similar conditions to those contained in prior years' OIG reports.

Department 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.

In addition to recommendations we made in the FY 2011 FISMA report, we are making 22 new recommendations to the OCIO to assist the Department in establishing and sustaining an effective information security program—one that complies with FISMA, OMB, and National Institute of Standards and Technology requirements. These recommendations supplement those made in another OIG report issued earlier in the year.[3]

OCIO concurred with 14 of the 22 recommendations (4.1, 7.1, 8.1, 8.2, 8.3, 8.6, 8.7, 9.1, 9.2, 9.3, 9.6, 9.7, 9.8, and 9.9), partially concurred with 6 of the 22 recommendations (4.2, 4.3, 4.4, 8.8, 9.4, and 9.5), and did not concur with 2 recommendations (8.4 and 8.5) contained in the draft report. We summarized and responded to specific comments in the "Audit Results" section of the audit report. We considered the OCIO's comments but did not alter or revise our findings or recommendations. OCIO declined to have an exit conference and chose to address the report through written comments.

[3] "Educational Central Automated Processing System (EDCAPS) Information Security Audit,", September 7, 2012 (ED-OIG/A11M0002).

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 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 (that is, 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 Connection 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 cybersecurity 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 cybersecurity with respect to the Federal information systems that fall within FISMA.

DHS updated the Inspector General reporting metrics for FY 2012 to include one-to-one mapping of the chief information officer's (CIO) metrics, allowing the Inspectors General to determine the progress of the control areas on which the CIOs report. DHS introduced this change to ensure the Inspectors General 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, CIOs, and Inspectors General. 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 CIO 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 Inspector General 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 April 5, 2012, the Department reported an inventory of 208 IT systems. For FY 2012 FISMA reporting, we judgmentally selected 16 of the Department's systems for review. Of the 16 systems selected, we included 4 from the judgmental sample performed as part of our FY 2011 FISMA review. We selected these systems to measure progress from the prior fiscal year. We selected the remaining 12 systems from the reported IT systems inventory based on the system impact level[4] of moderate or high from the Department's principal office components that managed the greatest number of systems.[5] We reviewed specific aspects of security controls for the sample, including risk management, system authorization, configuration management, and contingency planning.

[4] FIPS Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004, provides the definitions of potential impact levels. The potential impact is moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, assets, or individuals. The potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, assets, or individuals.
[5] The remaining 12 systems were selected from the following principal offices in the Department: FSA, Institute of Education Sciences; Office for Civil Rights; Office of Management; Office of Postsecondary Education; Office of Planning, Evaluation, and Policy Development; and Office of Special Education and Rehabilitative Services.

According to Gartner's IT Key Metrics Data, published in 2010, businesses spend an average of 5 percent of their total IT budget on IT security.[6] As of August 31, 2012, the Department had spent a total of $507 million on IT investments for FY 2012. The Department budgeted $12.5 million (about 2.5 percent of its total budget) for FY 2012 for IT security and FISMA compliance costs.

In September 2007, the Department entered into a contract with Dell Services Federal Government (DSFG) to provide and manage all IT infrastructure services to the Department under the Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) system.[7] The contract established a contractor-owned and contractor-operated IT service model for the Department under which DSFG 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, DSFG 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. 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 Education Network Infrastructure System (EDNIS), EDUCATE Mass Storage System (EDMASS), EDUCATE Security Operations Center (EDSOC), Department of Education's Central Automated Processing System (EDCAPS), EDUCATE Data Center Information System, and 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 CIO 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 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 DSFG and is located at the contractor 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.

[6] "How Much Should You Spend on IT Security," September 2010 (www.infoworld.com)
[7] Perot Systems (now DSFG) was acquired by Dell in September 2009.

AUDIT RESULTS

In March 2012, DHS prepared the Inspector General reporting metrics, or controls areas, for the FY 2012 FISMA review. The intent of the FY 2012 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 2012 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 them to be compliant in 3 of the 11 reporting metrics (Continuous Monitoring, Contractor Systems, and Security Capital Planning). However, we also identified findings in eight of the reporting metrics. The findings in six of the reporting metrics— Configuration Management, Identity and Access Management, Risk Management, Security Training, Remote Access Management, and Contingency Planning—were either repeat or modified findings from OIG reports issued from FY 2009 through FY 2011. We answered the questions in the DHS metrics template that will be input to the CyberScope FISMA Report as shown in Enclosure 1.

As part of this year's FISMA review, we incorporated results and findings from one audit report performed by an OIG contractor, "Education Central Automated Processing System (EDCAPS) Information Security Audit," September 7, 2012 (ED-OIG/A11M0002). The recommendations made by this FY 2012 FISMA review are in addition to those made in the EDCAPS audit report.

We also identified several prior year OIG reports that had similar or repeat findings to this year's audit fieldwork. These reports included:

- "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 (ED-OIG/A11I0006).

In its response to our draft report, OCIO concurred or partially concurred with the findings and recommendations in the report, with the exception of Finding Issue 8c, Recommendations 8.4 and 8.5. Specifically, OCIO disagreed with Reporting Metric Issue 8c that the two-factor authentication exemption process needed improvement. 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.

OCIO declined to have an exit conference and chose to address the report through written comments.

Management Response to the Overall Report

OCIO stated that the draft audit report underscores the need to ensure that corrective actions are addressed to resolve the noted issues with several of the reporting metrics. OCIO will work closely with OIG to manage the response activities appropriately. OCIO noted that of the 11 controls the OIG audited, OCIO placed increased emphasis on its Continuous Monitoring program and its Security Capital Planning activities (OIG found that these specific controls were in compliance with existing requirements in 2012). OCIO believes this emphasis was an appropriate and prudent response maximizing the overall effect of its efforts to improve the security of Department's information and IT systems, given available resourcing for its IT security and FISMA compliance programs. OCIO plans to leverage improvements in these control areas to justify increased investment in the Department's IT security and FISMA compliance programs in order to align such investments more closely with key metrics published by Gartner and others.

REPORTING METRIC NO. 1—Continuous Monitoring Management

FISMA FY 2012 Audit Results

The Department complied with this reporting metric. The OCIO established an entity-wide continuous monitoring program that assesses the security state of information systems that is consistent with OMB policy, FISMA requirements, and applicable NIST guidelines. For example, the Department adopted and was using several automated scanning and detection tools to collect, analyze, and report on security-related risks, issues, and threats to the Department. We found that, consistent with Continuous Monitoring reporting metrics, the Department's continuous monitoring program 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 (Repeat Finding)

FISMA FY 2012 Audit Results

The Department did not fully comply with this reporting metric.

Issue 2a. Patch Management Program Needs Improvement (Repeat Finding)

The OCIO had not established and implemented formal, enterprise-wide patch management policies and procedures consistent with NIST requirements. Although the OCIO had begun developing the vulnerability and patch management policy, the policy was still in draft form as of May 2012 when the document was requested. NIST Special Publication (SP) 800-53, Revision 3, Configuration Management-3, "Configuration Change Control and System," requires agencies to timely implement configuration control changes, such as remediating flaws, and to promptly install security-relevant software updates. Without effective patch management policies and procedures that ensure security patches are tested and installed in a timely manner, the Department increases the risks that unauthorized activities may occur and increases the potential that sensitive Department data may be released, used, or modified.

Issue 2b. Access Switch Port Security Needs Improvement (Repeat Finding)

The OCIO had not established access switch port security for the switches within the enterprise network infrastructure, nor did it disable unused switch port connections.[8] We tested switch port security by successfully connecting a rogue computer to one Departmental local-area network connection at a Department regional office. During the test, OIG auditors installed a five-port CISCO switch on a local-area network that was not detected or shutdown. The OCIO and DSFG did not prevent or detect a rogue device from being connected to the enterprise network infrastructure. NIST and the "Defense Information Systems Agency Network Security Checklist (CISCO Layer 2 Switch)" require that information systems have all access switch ports secured.[9] According to OCIO officials, the Department still has not established and implemented port security for unused ports, which the OIG identified and recommended to be addressed in the FY 2011 FISMA report. Eliminating unauthorized access to the network from inside the enterprise is vital to keeping a network secure from introducing a virus, spyware, and malware.

Final Reports Issued During 2012

In the EDCAPS audit report, the team found that the Department's configuration management controls over EDCAPS needed improvement.[10] Specifically, the OCIO had not implemented sufficient monitoring and oversight controls enterprise-wide to ensure prior OIG recommendations were implemented to address patch management control deficiencies.

---

[8] Switch port security consists of software settings that control authorized access from the ports to the switches.
[9] 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, 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.
[10] See report ED-OIG/A11M0002.

Final Reports Issued From FY 2009 Through 2011 Relating to Configuration Management

In addition to the FY 2011 FISMA audit, OIG has consistently reported configuration management issues in audits dating back to FY 2009.[11]

Recommendation

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

Management Response

OCIO concurred with the finding.

REPORTING METRIC NO. 3—Identity and Access Management (Repeat Finding)

FISMA FY 2012 Audit Results

The Department did not fully comply with this reporting metric. The OCIO had not fully developed processes for identity and access management. Specifically, we found that the OCIO did not establish policies and procedures to identify all devices that were attached to the network, distinguish those devices from users, and authenticate devices that were connected to the network. NIST SP 800-53, Revision 3, IA-2, "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. The OCIO still has not established and implemented policies and procedures to be consistent with NIST requirements for establishing and maintaining an effective Identity and Access Management program.

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, 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. 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.

[11] See reports ED-OIG/A11L0001, A11J0006, and A11I0006.

Although the OCIO did not establish and implement policies and procedures to be consistent with NIST requirements for establishing and maintaining an effective identity and access management program, OCIO took steps to build and develop this function. For instance, the OCIO:

- awarded the enterprise security architecture task order,
- engineered a study on the implementation life cycle support required to integrate and operate a Network Access Control device, and
- planned to use the results from the study to establish the identity and access management procedures by December 31, 2012.

Final Reports Issued From FY 2009 Through 2011 Relating to Identity and Access Management

The current identity and access management condition was also identified during our FY 2011 FISMA audit. In addition to the FY 2011 FISMA audit, the OIG reported identity and access management issues in a previous audit for FY 2009.[12]

Recommendation

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

Management Response

OCIO concurred with the finding.

REPORTING METRIC NO. 4—Incident Response and Reporting

FISMA FY 2012 Audit Results

The Department did not fully comply with this reporting metric. Specifically, FSA did not consistently and effectively respond to keylogger incidents.[13] FSA's Information System Security Officers (ISSO) did not consistently review the system event audit logs for all compromised privileged account incidents.[14] In calendar year 2011, FSA reported 647 compromised privileged accounts. However, only 41 (6 percent) of those accounts had audit log reviews performed by the ISSO. Further, in 2012, FSA reported 172 compromised privileged accounts. However, only 101 (59 percent) of those accounts had audit log reviews performed by the ISSO. Although FSA demonstrated improvement in the review of system audit logs for compromised privileged accounts from calendar year 2011 to 2012, ISSOs were still not reviewing all the compromised privileged account incidents in accordance with FSA

[12] See report ED-OIG/A11L0001.
[13] Keylogging is a method of capturing and recording user's keystrokes.
[14] "Federal Student Aid Keylogger Incident Response Standard Operating Procedures," April 2011, states, at a minimum, the audit logs are reviewed for (1) unusual or multiple logon internet protocol addresses, (2) unusual logon times or dates, and (3) unusual account activity.

procedures.[15] NIST SP 800-61, Revision 2, "Computer Security Incident Handling Guide," requires organizations to create incident response policies and plans, develop procedures for performing incident handling and reporting, and establish logging standards and procedures to ensure that adequate information is collected by logs and security software and the data is reviewed regularly.

FSA identified certain program limitations in its effort to respond to keylogger incidents. For instance, (1) there are no dedicated positions to address keylogging issues, (2) resources available to review audit logs are limited, (3) ISSOs need comprehensive training on how to review logs, and (4) some contracts do not include a requirement to provide audit logs to FSA. The inability to perform a log review of all compromised privileged account holders could give unauthorized users access to privileged Department information that could have severe adverse effects on the organization's operations, assets, or individuals.

Final Reports Issued During 2012

The EDCAPS audit team found that OCIO has not established and implemented effective controls to review, reconcile, track, report, and resolve G5 keylogger incidents entered into Operational Vulnerability Management System to ensure compliance with NIST 800-53, Revision 3 guidance.

Final Reports Issued From FY 2009 Through 2011 Relating to Incident Response and Reporting

We also identified incident response and reporting issues in the FY 2011 EDUCATE report.[16] Specifically, OCIO was not in compliance with NIST requirements to report security incidents to the United States Computer Emergency Response Team within required timeframes. Further, OCIO did not resolve security incidents in a timely manner to prevent further damage. In addition to the EDUCATE audit, the OIG's Technology Crimes Division reported 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. The OIG reported incident response and reporting issues in a previous audit for FY2009.[17]

Recommendations

We recommend that OCIO:

4.1 Review logs for the remaining 606 and 72 compromised privileged accounts from calendar year 2011 and 2012, respectively.

[15] "FSA Keylogger Incident Response Standard Operating Procedures," April 2011.
[16] The results of the FY 2011 EDUCATE report were cited as support in our FY 2011 FISMA report.
[17] See report ED-OIG/L21K0002.

4.2 Enforce the requirement for ISSOs to perform a log review of all compromised privileged accounts to ensure incidents are properly remediated in accordance with "FSA Keylogger Incident Response Standard Operating Procedures."

4.3 Ensure that ISSOs receive proper training so they can properly review system event audit logs for compromised privileged accounts.

4.4 Review and amend or modify all contracts (as applicable) to have audit logs provided to FSA and require ISSOs to perform log reviews of compromised privileged accounts.

Management Response

OCIO concurred with the Recommendation 4.1 and partially concurred with Recommendations 4.2, 4.3, 4.4.

For Recommendations 4.2, 4.3, and 4.4, OCIO stated that although FSA believes the recommendations are alternative approaches that could be used, it has implemented an alternative approach that it believes is more effective. FSA contracted with an independent security review team to complete log reviews for all privileged user account compromises identified through analysis of files provided by US-CERT.

For Recommendation 4.2, OCIO agreed to convert the "FSA Keylogger Incident Response Standard Operating Procedures" into a Department-wide process and update it with the approach for centralized support by May 15, 2013.

For Recommendation 4.3, OCIO stated that although FSA's approach to satisfy this finding and recommendation differ from OIG's recommendation, FSA agreed with OIG that ISSOs should be trained to complete the log reviews as recommended and will provide training during its monthly ISSO meetings to ensure ISSOs complete this activity. The training will be completed by September 15, 2013.

For Recommendation 4.4, OCIO stated that FSA concurred that all contracts should be reviewed to determine contract responsibility for log submissions. Once gaps are identified, FSA plans to work with its business units to modify or amend contracts. Contract expiration dates and cost will be used to determine best alternatives. However, FSA does not concur with the recommendation to require that ISSOs perform log reviews and will follow the alternative approach described above regarding the independent security review team. The contractor's work will be reviewed to assess fidelity of implementation and implications of log reviews by September 15, 2013.

OIG Response

The OIG agrees with FSA's proposed alternative approach and corrective action to remediate the identified Incident Response and Reporting findings. However, OCIO's response was unclear regarding whether ISSOs will perform system event audit logs for compromised privileged accounts. For management's response to Recommendation 4.3, OCIO states that "FSA agrees with OIG that ISSOs should be trained to complete the log reviews as recommended and will provide training during its monthly ISSO meetings to ensure ISSOs complete this activity."

However, in management's response to Recommendation 4.4, OCIO states that "FSA does not concur with the recommendation to require ISSOs to perform log reviews." FSA needs to clarify whether reviewing system event audit logs for compromised privileged accounts will be part of the ISSO job function in addition to the independent security review team reviews. OIG requests quarterly updates to determine the status of the above corrective actions.

REPORTING METRIC NO. 5—Risk Management

FISMA FY 2012 Audit Results

The Department did not fully comply with this reporting metric.

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

OCIO has still not fully implemented the 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. 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. The OCIO did not fully update and implement 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.

Although OCIO had not finalized risk management policies and procedures to incorporate changes in NIST SP 800-37, Revision, 1, the OCIO took a number of steps to build and develop the Department's risk management program. For instance, the OCIO:

- implemented an enterprise capability that assesses operational risk associated with all network assets and provides the Department's leadership with situational awareness;
- provided required information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, arising from the operation and use of information systems;
- established a security engineering group under the chief information security officer to guide and direct risk through the system development life cycle; and
- developed the draft IT Security Risk Management guidance.

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 April 5, 2012, the Department reported a total of 208 systems in its inventory. The inventory consisted of 61 Departmental systems, 109 contractor-owned systems, and 38 systems with no identified affiliation.[18] For these 208 systems, we identified that:

- 49 (23 percent) were operating on expired security authorizations,
- 74 (35 percent) were operating on expired self-assessment dates, and
- 110 (53 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 208 systems. For the 16 systems judgmentally selected to review, we found:

- 4 systems were operating on expired security authorizations,
- 1 system did not have a consistent FIPS Publication 199 system categorization level for its system security plan and FISMA FY 2012 inventory listing,
- 1 system had a security assessment report that expired,
- 1 system did not have a security assessment report or related POA&M, and
- 2 systems had system security plans that were not updated within the required 3-year security authorization period.

According to OCIO officials, several systems in the FY 2012 inventory had system documentation that was either missing or had inaccurate information within the Operational Vulnerability Management System. 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 the 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 on an ongoing basis 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 During 2012

The EDCAPS audit team found that the Department did not perform and document the required EDCAPS and G5 security assessments in accordance with NIST and Departmental guidance. Specifically, OCIO did not have formally approved risk assessment documentation before migrating Phase 3 of G5 into production. Additionally, a revised authorization to operate letter was not found for G5 Phase 3 installation.

[18] The system was neither identified as a Departmental system nor contractor-owned system.

Final Reports Issued From FY 2009 Through 2011 Relating to Risk Management

We identified similar risk management issues in our FY 2011 FISMA audit. Specifically, OCIO did not timely implement a risk management program consistent with NIST SP 800-37, Revision 1.[19] 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 2011 FISMA audit, the Department reported issues with risk management in audits dating back to FY 2009.[20]

Recommendation

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

Management Response

OCIO partially concurred with the recommendations from the FY 2011 FISMA report (ED-OIG/A11L0003). For Recommendation 5a, although OCIO has not updated OCIO-01 or OCIO-05 to include Risk Management, OCIO published "Information System Security Authorization Guidance," on June 15, 2011. This guidance includes a comprehensive governance structure and organization-wide risk management strategy with techniques and methodologies that the Department will employ to assess information system-related risk and to preserve availability, confidentiality, and integrity. OCIO stated that this guidance also addressed Recommendation 5b. The guidance is consistent with NIST SP 800-37 and provides documentation of a common controls document. OCIO will complete a comprehensive risk management implementation plan including policies and procedures by September 30, 2013.

OIG Response

Although OCIO has taken several steps with regard to the corrective actions for recommendations discussed in the FY 2011 FISMA report, OCIO still has not fully developed and implemented a risk management program in accordance with NIST SP 800-37. OIG requests quarterly updates to determine the status of the above corrective actions.

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

FISMA FY 2012 Audit Results

The Department did not fully comply with this reporting metric. The OCIO 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 and

[19] "Guide for Applying the Risk Management Framework for Federal Information Systems," February 2010.
[20] See report ED-OIG/A11L0001.

training before they are allowed access to the systems.[21] 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. While we were able to determine that OCIO developed a Web site to address A-130 security requirements using the Department's onboarding process for new employees and coordinated that effort with another principal office, OCIO has yet to implement the new 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, recognize IT security situations, and take appropriate steps to avert them. For the Department's programs to achieve their objectives, each individual user of the Department's IT resources needs to assume responsibility for IT security.

Final Reports Issued From FY 2009 Through 2011 Relating to Security Training

We also identified the current security training condition in our FY 2011 FISMA audit.

Recommendation

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

Management Response

OCIO stated that it resolved the prior report's recommendation in July 2012. OCIO, in conjunction with its security awareness and training support contractor, developed a "New Employee Cyber Security and Privacy Orientation" course that is provided as part of the Department's Corporate Onboarding Process, EDStart on-line, and is posted on the Department's Web site. All new Department employees are required to complete this course in advance of reporting onboard, and they must provide proof of course completion when they report for employee orientation. In addition, OCIO updated and improved the Department's annual security awareness training material, consolidating information security with privacy training. OCIO stated that it also continues to hold annual security awareness training activities and events during the DHS October Cybersecurity Awareness Month.

OIG Response

As of May 2012, OCIO did not provide evidence that corrective action was taken for the FY 2011 FISMA report recommendations. However, since then, OCIO has developed a security awareness and training course that employees are required to complete as part of the Department's Corporate Onboarding Process. Once completed, employees are required to

[21] OMB Circular A-130, Appendix III, November 28, 2000, as clarified by 5 C.F.R. § 930.301and NIST SP 800.53, Revision 3, August 2009.

provide documentation of completion before employee orientation to Human Capital and Client Services and OCIO. However, we confirmed that Human Capital and Client Services and OCIO currently do not retain this documentation. Therefore, we cannot verify that the employees completed the required training.

REPORTING METRIC NO. 7—Plan of Action and Milestones

FISMA FY 2012 Audit Results

The Department did not fully comply with this reporting metric. The OCIO did not have fully documented procedures for the POA&M process. Specifically, the OCIO did not update the POA&M standard operating procedures to include the processes and procedures for informing management when POA&M milestones are not met.[22] NIST SP 800-53, Revision 3, requires organizations to implement a process for ensuring that POA&Ms for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the nation. Without fully documented POA&M procedures, OCIO misses the opportunity to accurately respond and implement needed actions to mitigate identified security risks to information systems.

Final Reports Issued From FY 2009 Through 2011 Relating to Plan of Action and Milestones

We have identified POA&M issues in previous OIG reports. For instance, according to the FY 2011 EDUCATE report, OCIO did not adequately manage the POA&M process because it did not (1) maintain an accurate inventory, (2) provide all security weaknesses from its dashboard to management, (3) monitor all security weaknesses in the POA&M reports and audit dashboard, and (4) report security weaknesses identified during monthly network vulnerability scans.

Recommendation

7.1 We recommend that OCIO update the current POA&M procedures to include the processes and procedures for informing management when POA&Ms are not met.

Management Response

OCIO concurred with the recommendation.

REPORTING METRIC. NO. 8—Remote Access Management

FISMA FY 2012 Audit Results

The Department did not fully comply with this reporting metric.

[22] Referred to as stoplight charts by OCIO.

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

OCIO still does not have a detailed or comprehensive telework security policy that reflects Federal guidance to protect information systems and the data that reside on these systems. In response to the FY 2011 FISMA report, OCIO developed a Telework Security Guidance document, which was scheduled to be disseminated by May 2012. However, OCIO did not meet the deadline for issuance and the draft document was still awaiting final approval. 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 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 followed properly.

Issue 8b. FirePass and Citrix Did Not Time Out After 30 Minutes of Inactivity (Repeat Finding)

Access through FirePass and Citrix did not time out after 30 minutes of inactivity. As part of our audit fieldwork, we performed testing using government-furnished equipment (GFE) and non-GFE equipment and found that FirePass and Citrix still did not time out after 30 minutes of inactivity. OMB guidance requires agencies to use a time-out function for remote access and mobile devices requiring user reauthentication after 30 minutes of inactivity.[23] Although the OCIO adjusted the inactivity settings to time out after 30 minutes in response to the recommendation in the FY 2011 FISMA report, OCIO did not effectively test and verify the inactivity setting to ensure that it was working correctly. Without this setting, a user (especially one logged into a third party location) could expose the Department's networks and compromise the confidentiality, integrity, and availability of information and information systems.

Issue 8c. Two-Factor Authentication Exemption Process Needs Improvement

OCIO did not have established and documented policies and procedures for managing users who were exempt from dual authentication (two-factor authentication) when accessing the Department's network remotely. Specifically, OCIO and DSFG officials were unable to provide justification for allowing users to access the Department's network with single-factor authentication, who were deemed exempt from dual authenticating.[24] OMB Memorandum M-05-24, "Implementation of Homeland Security Presidential Directive 12 – Policy for a

[23] OMB M-06-16, "Protection of Sensitive Agency Information" and OMB M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information."

[24] According to OCIO officials, this is determined on a case-by-case basis. Each individual's access requirements are assessed to determine whether the user is deemed eligible to be exempt from dual authentication when accessing the network remotely.

Common Identification Standard for Federal Employees and Contractors," August 5, 2005, requires Federal agencies to use multifactor authentication for access to information systems by October 27, 2005. Two years later, OMB provided additional guidance for two-factor authentication for remote access.[25] According to OCIO officials, the Department accepted the risk involved with allowing single-factor authentication for Department employees with special requirements who are unable to dual authenticate when accessing the Department network. OCIO officials also stated that there were no current policies and procedures in place for the management of users who have been deemed exempt from dual authenticating to connect to the network. OCIO's current exemption process could allow any user (not on the exemption list) to bypass the dual-authentication process.

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

OCIO had not fully implemented and enforced the use of two-factor authentication when accessing the Department's systems to comply with DHS and OMB guidance requiring two-factor authentication. The Department was still in the process of implementing and enforcing the use of two-factor authentication for all Federal employees, contractors, and other authorized users. According to FSA officials, guaranty agency users have not been configured to dual authenticate. Specifically, FSA officials were not scheduled to disseminate tokens to about 300 users from 36 guaranty agencies until the end of FY 2012. In addition, OCIO officials stated that dual authentication for webmail had not been implemented due to technical limitations of the current infrastructure. However, OCIO was in the process of determining how to implement a solution in the near future. Allowing users to sign on without two-factor authentication could expose user accounts and lead to cyber-attacks.

Issue 8e. Citrix Inventory Process Needs Improvement

OCIO did not document and maintain a complete list of active servers on the Citrix infrastructure for EDUCATE. Additionally, by analyzing Citrix security logs, we determined that numerous servers logging into the network were not accounted for in the EDUCATE infrastructure diagram provided to the OIG.[26] NIST SP 800-53, Revision 3, "Configuration Management," requires agencies to develop, document, and maintain an inventory of information system components that (1) accurately reflects the current information system, (2) is consistent with the authorization boundary of the information system; (3) is at the level of granularity deemed necessary for tracking and reporting, (4) includes organization-defined information deemed necessary to achieve effective property accountability, and (5) is available for review and audit by designated organizational officials. We found a lack of documentation to support the current Citrix infrastructure for EDUCATE. It is imperative that all servers are accounted for in the Department's overall infrastructure to ensure that appropriate patch management is performed, new security requirements and regulatory mandates are followed, and servers are accounted for regarding disaster recovery purposes. Also, by maintaining an accurate and up-to-date listing of servers in production, the Department will ensure that all servers are accounted for in backup recovery procedures.

[25] OMB M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 22, 2007.
[26] A security log is a log that contains records of login and logout activity or other security-related events specified by the system's audit policy.

Issue 8f. Configuration of Non-Government-Furnished Equipment Process Needs Improvement

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 DSFG 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.

Final Reports Issued From FY 2009 Through 2011 Relating to Remote Access Management

We identified remote access management issues in our FY 2011 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, OIG has consistently reported remote access management issues in audits dating back to FY 2009.[27]

Recommendations

We recommend that OCIO:

8.1 Validate the changes to the FirePass inactivity settings to ensure sessions are timing out after 30 minutes of inactivity.

8.2 Distribute dual-authentication tokens to all guaranty agency users and all other external business partners with privileged accounts in order to comply with OMB and NIST mandates.

8.3 Configure webmail to require dual authentication as mandated by OMB-06-16 and OMB-07-16, or allow email to be accessible only via FirePass sessions that use dual authentication.

8.4 Develop written policies and procedures to define the dual-authentication exemption requirements and process.

[27] See reports ED-OIG/A11L0001, L21K0002, and A11I0006.

8.5 Formally document the Department's position to accept the risk to allow single-factor authentication for those individuals who meet the exemption requirements.

8.6 Update the telework policy requirements to perform validation procedures to ensure the security of non-GFE devices used to connect to the Department's network remotely.

8.7 Ensure that a complete inventory is documented and maintained that accurately accounts for all Citrix servers used in the production environment, and ensure that changes are made in a timely manner to accurately represent the current overall infrastructure.

8.8 Identify and maintain tracking of teleworkers who use non-GFEs to connect to the network remotely and ensure those devices have been configured to the standards set forth in the telework requirements.

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

Management Response

OCIO concurred with Recommendations 8.1, 8.2, 8.3, 8.6, and 8.7 did not concur with Recommendations 8.4 and 8.5, and partially concurred with Recommendation 8.8.

For Recommendations 8.4 and 8.5, OCIO stated that remote access through Firepass requires dual authentication and no exemptions are allowed. As such, no policy or procedures is required. If it determines an exemption is applicable and appropriate, OCIO will develop the corresponding policies, procedures, and processes for managing.

For Recommendation 8.8, OCIO stated that in response to identifying and maintaining tracking of teleworkers who use non-GFEs to connect to the network remotely, the Department's telework policy (Flexiplace Work Agreement) requires employees provide asset information on the IT equipment they will use to conduct their telework activities. Employees are also notified of the expectations for applying approved safeguards to protect Government and agency records from unauthorized disclosure or damage. Further, OCIO stated that the Department may not be able to ensure non-GFE devices have been configured to standards set forth in the telework requirements because of problems with the legality of the Department treating non-GFE as if it were a GFE. To declare that only GFE devices may connect to and work on the Department's networks and systems would necessitate an enormous outlay of funding to purchase GFE for anyone wishing to telework, and this is currently not a feasible solution. OCIO has been investigating endpoint inspection capabilities as a means of checking devices for compliance with GFE standards. OCIO stated it does not yet know whether this is a viable solution, but it will continue to keep OIG apprised of its progress on this issue.

OIG Response

For Recommendation 8.4 and 8.5, although OCIO stated that dual authentication is required for remote access through FirePass, our interviews with OCIO personnel indicated that there were users who have the capability to authenticate but were exempt from dual authenticating under

certain requirements. OCIO provided detailed information citing the users who were deemed exempt from dual authenticating, but when we requested policies and procedures governing the exemption requirements and process, OCIO did not provide that information. Further, the OIG recommended additional documentation to formally support the Department's position to accept the risk to allow single-factor authentication for those individuals who meet the exemption requirements.

For Recommendation 8.8, OCIO did not provide evidence that the Departmental telework policy (Flexiplace Work Agreement) and notifications about using non-GFE are consistently implemented and teleworkers who use non-GFEs are identified and tracked to ensure those devices have been configured to the standards set forth in the telework requirements.

OCIO should provide a specific corrective action that it will take to ensure non-GFE devices are configured to the standards set forth in the telework requirements and provide an expected timeframe of when a viable solution would be implemented.

REPORTING METRIC NO. 9—Contingency Planning

FISMA FY 2012 Audit Results

The Department did not fully comply with this reporting metric.

Issue 9a. Contingency Plans Not Complete (Modified Repeat Finding)

OCIO relied on contingency plans that were not complete. Specifically, 14 of 16 system contingency plans we reviewed did not include all the required contingency planning elements identified in NIST and Departmental guidance.[28] For example, we found that some contingency plans did not (1) document defined training requirements, (2) identify an alternate storage site for system backups, (3) identify procedures regarding the frequency of system backups, or (4) identify the alternate telecommunication services. This occurred because OCIO did not ensure contingency plans were complete to include 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.

Issue 9b. Contingency Plan Testing Process Needs Improvement

OCIO did not consistently perform and document contingency plan testing in accordance with NIST guidelines and Departmental guidance. For 2 of the 16 systems, we did not find supporting documentation to validate the annual testing of the systems' contingency plan. Specifically, we found that the contingency plans for the National Household Education Survey System and for

[28] 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.

the Higher Education Programs Field Reader System were last tested in January 2011, and April 2011, respectively. NIST SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems," states that testing is a critical element of a viable contingency capability and enables plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan. OCIO-01, "Handbook for Information Assurance Security Policy," requires all contingency plans for systems to be tested annually and the results of the tests documented and used to update the contingency plan and POA&M items created as a result, if necessary.

Additionally, for the same two systems referenced above, OCIO officials were unable to furnish the documented contingency plan test results. OCIO officials are not consistently requiring ISSOs or system owners to perform and document contingency plan tests for all the Department systems in accordance with NIST guidelines and Departmental procedures. If the Department does not perform and document contingency plan tests, it is unable to validate recovery capabilities and identify or correct the deficiencies in the contingency plans. In addition, the Department is unable to validate that recovery procedures are in place and personnel have the capability to effectively recover Departmental systems in the event of a disaster.

Issue 9c. Principal Offices' Business Continuity Plans Need To Be Updated

The Department's principal offices relied on business continuity plans (BCP) that were missing required elements per the Department's BCP template.[29] Specifically, 6 out of 8 principal office BCPs did not include all the required BCP elements. For example, the BCPs did not include all of the required emergency contact information for the essential business continuity personnel who would be contacted in the event of an emergency. OM 5-102, "Continuity of Operations," requires that each principal office develop a BCP in coordination with the continuity manager to ensure that its BCP addresses and adheres to mission critical functions outlined in the continuity plan. The BCP should focus on the recovery of the principal office's mission critical and essential business processes within headquarters and all regions.

OCIO did not effectively and consistently provide guidance about and oversight of principal offices for the development of the BCPs to ensure completeness and accuracy of the information consistent with the Department's BCP template. Without complete BCP information, essential personnel will not be able to effectively recover the critical and essential business processes that principal offices identified. Further, Department personnel will not be able to resume business functions in the event of an emergency or other situation that disrupts or threatens to disrupt operations for a prolonged period.

Issue 9d. Business Impact Analysis Process Needs Improvement (Modified Repeat Finding)

The Department did not consistently perform a Business Impact Analysis (BIA) for all its systems in accordance with NIST guidelines and Departmental procedures.[30] Specifically, 6 of

[29] A BCP focuses on sustaining an organization's mission and business functions during and after a disruption. A BCP may be written for mission and business functions within a single business unit or may address the entire organization's processes.

[30] 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.

16 systems' contingency plans we reviewed did not have support documentation to validate the completion of a BIA. OCIO did not effectively and consistently ensure that the ISSOs or system owners were completing and documenting a BIA as part of the development of their system contingency plans. OCIO officials stated that the BIAs for each EDUCATE-supported system are still being developed. By not performing and documenting a BIA, the Department is unable to identify and prioritize information systems and components critical to supporting the Department's mission and business functions. Further, a BIA helps prioritize the systems and processes based on the FIPS Publication 199 impact level and helps prioritize recovery strategies to minimize loss.

Issue 9e. Information Systems Contingency Plans Not Documented

During our review of the system documentation for the 16 judgmentally selected systems, we found that OCIO and FSA had not established a separate information system contingency plan for the EDUCATE Mass Storage System (EDMASS), EDUCATE Network Information System (EDNIS), EDUCATE Security Operations Center (EDSOC), and Direct Loan Consolidation System (DLCS) in accordance with NIST guidelines and Departmental procedures.[31]

According to OCIO officials, the EDUCATE disaster recovery plan serves as the information system contingency plan for EDMASS, EDNIS, and EDSOC. However, a disaster recovery plan and an information system contingency plan are different in that the disaster recovery plan addresses only information system disruptions that require relocation. NIST SP 800-34, Revision 1, "Contingency Planning for Federal Information Systems," May 2010 states that a disaster recovery plan is not the same as a contingency plan. Contingency plan procedures are developed for recovery of the system regardless of site or location. An information system contingency plan can be activated at the system's current location or at an alternate site. In contrast, a disaster recovery plan is primarily a site-specific plan developed with procedures to move operations of one or more information systems from a damaged or uninhabitable location to a temporary alternate location. A disaster recovery plan may support a BCP by recovering supporting systems for mission and business functions or mission-essential functions at an alternate location.

In addition, FSA did not provide adequate oversight to ensure contractors followed Departmental policies and procedures requiring that all general support systems and major applications establish a system contingency plan. Information systems are vital elements in most mission and business functions. Information system resources are essential to an organization's success. It is critical that identified services provided by these systems are able to operate effectively without excessive interruption. Further, without proper contingency planning, systems may not be able to recover quickly and effectively following a service disruption or disaster.

Before we completed our fieldwork, FSA provided an approved DLCS information system contingency plan. Therefore, we will not make any recommendations regarding a contingency plan for that system.

[31] See footnote 30.

Issue 9f. Disaster Recovery Testing Process Needs Improvement

OCIO did not test Citrix servers as part of the annual disaster recovery testing of major applications and general support systems in accordance with NIST guidelines and Departmental policies and procedures.[32] OCIO did not consistently and effectively document the completion of disaster recovery test exercises performed for systems and applications that reside on the EDUCATE general support system. Specifically, the 2011 disaster recovery exercise results included Citrix in the list of servers to be tested during the exercise but did not include any test results for the Citrix servers. Because Citrix servers are essential in allowing users to remotely connect to Departmental systems, failure to test the servers increases the risk that users would not be able to access Departmental resources in the event of a disaster.

Final Reports Issued From FY 2009 Through 2011 Relating to Contingency Planning

We also identified contingency planning issues in the FY 2011 FISMA audit. Specifically, OCIO relied on contingency plans that were missing required elements identified in NIST and Department guidance.[33] In addition to the FY 2011 FISMA audit, OIG has reported contingency planning issues in audits dating back to FY 2010.[34]

Recommendations

We recommend OCIO:

9.1 Review and update information system contingency plans for the 14 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 Perform and document information system contingency plan test results for the National Household Education Survey System and Higher Education Programs Field Reader System as required by NIST guidelines and Departmental procedures.

9.3 Ensure ISSOs or system owners perform annual contingency plan testing and document test results as required by NIST guidelines and Departmental procedures.

9.4 Develop and maintain individual information system contingency plans and disaster recovery plans for EDMASS, EDNIS, and EDSOC.

9.5 Update Departmental policies and procedures to define the requirement for the consolidation of general support systems and major application contingency plans and disaster recovery plans as part of contingency planning procedures.

[32] See footnote 30.
[33] 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.
[34] See reports ED-OIG/A11J0006 and A11J0001.

9.6 Ensure ISSOs or system owners perform and document a BIA as part of contingency planning for all systems in accordance with NIST guidelines and Departmental procedures.

9.7 Develop Citrix recovery procedures to use during disaster recovery testing, and document the results of test performed.

9.8 Require principal offices to update the BCPs for the six systems that have elements missing (list provided to OCIO) to ensure that all the required BCP elements are included in accordance with the Department's BCP template.

9.9 Review the remaining principal offices' BCPs for completeness and accuracy to ensure they are in accordance with the Department's BCP template.

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

Management Response

OCIO concurred with Recommendations 9.1, 9.2, 9.3, 9.6, 9.7, 9.8, and 9.9 and partially concurred with Recommendation 9.4 and 9.5. For Recommendation 9.4, OCIO stated that in FY 2012, EDMASS and EDNIS were combined into a single security boundary called Infrastructure, which has a contingency plan and disaster recovery plan separate from the other EDUCATE security boundaries. The contingency and disaster recovery plans for each security boundary will be uploaded in OVMS by December 31, 2012. For Recommendation 9.5, OCIO stated that the current "Information System Security Authorization Guidance," which was issued in June 2011, specifically refers to a contingency plan as including "procedures for the assessment and recovery of a system following a system disruption," which covers both contingency planning and disaster recovery.

OIG Response

For Recommendation 9.4, although OCIO stated that EDMASS and EDNIS were combined into a single Infrastructure security boundary, when we requested the contingency and disaster recovery plans for our sample of 16 systems in April 2012, OCIO did not provide an Infrastructure contingency plan and disaster recovery plan, nor did it provide a separate contingency or disaster recovery plan for EDSOC. For Recommendation 9.5, our recommendation was based on information the OCIO provided at the time of our request. OCIO stated at that time that the EDUCATE disaster recovery plan was the "overarching document that encompassed all the EDUCATE boundaries." The OCIO should update policies and procedures to define the circumstances when Department systems' and major applications' contingency and disaster recovery plans are consolidated into a single document.

REPORTING METRIC NO. 10—Contractor Systems

FISMA FY 2012 Audit Results

The Department fully complied with this reporting metric. As of April 2012, the Department's system inventory identified 109 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 that included the following attributes:

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

We also identified that the Department is in the process of implementing the continuous monitoring element to the security authorization process as the Department is transitioning to a continuous system authorization process. This would allow for additional system reviews on an annual basis and provide a near real-time depiction of systems' security postures.

Although no recommendations were needed for this reporting metric, the deficiencies identified in Findings 2 through 9 affect or apply to all Departmental systems, whether contractor-operated or agency-operated.

REPORTING METRIC NO. 11 – Security Capital Planning

FISMA FY 2012 Audit Results

The Department complied with this reporting metric. Specifically, the Department 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

As part of this year's FISMA audit work, DHS requested that we indicate the Department's progress in implementing recommendations to correct weaknesses identified in prior OIG audit reports. As part of our audit fieldwork, we identified OIG reports that were issued during fiscal years 2009 through 2011 to determine whether the Department has taken action in implementing the recommendations in those reports. The reports included:

- "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 (ED-OIG/A11I0006).

We found that the audits listed above contained 129 recommendations. We used the Audit Accountability and Resolution Tracking System to identify and review the corrective action plans for implementing each of the recommendations.[35] We reviewed the supporting documentation the OCIO provided to us to ensure that it was sufficient to demonstrate that the OCIO was taking or had taken corrective action with respect to each of the recommendations. As of August 29, 2012, the Audit Accountability and Resolution Tracking System showed that the Department had implemented 93 of the 129 recommendations, but the remaining 36 were still outstanding. Of the 36 recommendations, 19 were still within the original proposed deadline date for completing implementation. However, management had revised or extended the implementation dates for the remaining 17 recommendations. OCIO's resolving the remaining recommendations will ensure that the Department remediates previously identified security weaknesses and that the weaknesses will not occur as repeat or modified repeat findings in future OIG audit reports.

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

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine whether the Department's overall information technology security program and practices comply with the E-Government Act (Public Law 107-347) including Title III, FISMA, and Office of Management and Budget (OMB) guidance. Our review covered FY 2012. 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 questions DHS provided for the FY 2012 FISMA review, which are designed to assess the status of the Department's security posture in FY 2012. OMB issued the Inspectors General metrics, or controls areas, to be assessed for FY 2012 FISMA compliance in March 2012. For FY 2012 FISMA reporting, each Inspector General was required to evaluate their respective agency, based on DHS guidance, 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

For FY 2012 FISMA reporting, we judgmentally selected 16 systems for review. Of the 16 systems selected, we included 4 from prior year reviews that required followup due to recommendations made concerning deficiencies identified in system documentation. We selected these systems in order to measure progress from the prior fiscal year. We selected the remaining 12 systems from OCIO's FY 2012 Reportable Systems universe based on several factors. First, we focused on reviewing a system from each principal office, where possible, to ensure the review was not restricted to one specific office. Second, we identified and selected systems within each office that have at least a "moderate" impact level, based on FIPS Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," which identifies those systems that if compromised would have a serious adverse effect on organizational operations, assets, or individuals. Third, to ensure that we reviewed system documentation for both contractor-owned and Department-owned systems, we included systems owned by both entities. The table below lists the systems selected, the system's Principal Office, the FIPS Publication 199 potential impact level, and whether the system was

selected as a follow-up system from prior year reviews, or was a new selection as part of our FY 2012 review. We used this sample to evaluate the security areas of Configuration Management, Contingency Planning, Contractor Systems, and Risk Management. 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	Initial fiscal year Selection
1	EZ-Audit	FSA	High	2012
2	Central Processing System	FSA	Moderate	2012
3	Direct Loan Processing System	FSA	Moderate	2012
4	IES Data Center	IES*	Moderate	Followup
5	National Household Education Survey System	IES	Moderate	2012
6	Case and Activity Management System	OCR*	Moderate	2012
7	EDUCATE Mass Storage System	OCIO	High	Followup
8	EDUCATE Network Information System	OCIO	High	Followup
9	EDUCATE Security Operations Center	OCIO	High	Followup
10	FOIA Tracking and Reporting System	OM*	Moderate	2012
11	Higher Education Programs Field Reader System	OPE*	Moderate	2012
12	Jacob K. Javits Fellows Database	OPE	Moderate	2012
13	Teacher Education Assistance for College and Higher Education Grant Program SDC	OPE	Moderate	2012
14	BS Budget Formulation	OPEPD*	Moderate	2012
15	TRIM TRIO	OSERS*	Moderate	2012
16	National Center on Service Obligation Scholar Tracking System	OSERS	Moderate	2012

* Institute of Education Sciences; Office of Civil Rights; Office of Management; Office of Postsecondary Education; Office of Planning, Evaluation and Policy Development; and Office of Special Education and Rehabilitation Services.

In addition to our FISMA fieldwork, we incorporated the results of the "Education Central Automated Processing System (EDCAPS)," September 7, 2012 (ED-OIG/A11M0002), into this year's FISMA review.

EDCAPS Information Security Audit

This audit was performed by an independent contractor on behalf of the OIG. The purpose of this audit was to determine whether information technology security controls and effective management controls are in place to protect Departmental resources, including the safeguarding of personally identifiable information. The audit was limited to an assessment of the

effectiveness of the Department's overall information security program and practices for EDCAPS in accordance with the E-Government Act (Public Law 107-347), including Title III, the Federal Information Security Management Act of 2002, OMB, NIST regulations and standards. The audit team concluded that the Department's information systems security program controls over EDCAPS needed improvement to address seven operational, managerial, and technical security control risks.

The FY 2012 FISMA audit covered the Department's management of IT security programs and systems for FY 2012. It included Department-wide and IT system audits completed during FY 2012. Fieldwork was conducted from February 2012 through July 2012, primarily at Departmental offices in Washington, D.C., and Dallas, Texas, and contractor facilities in Washington, D.C., and Plano, Texas. Our evaluation of prior audit coverage and the Department's progress in implementing recommendations and correcting IT security weaknesses includes findings and reports issued during FY 2009 to the present. Although an exit conference was scheduled for September 27, 2012, OCIO declined to meet and addressed the findings and recommendations in written comments to the draft report.

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 or system output for information purposes only, so we did not assess the reliability of computer-processed data.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Enclosure 1: Cyberscope FISMA Reporting

Inspector General

Section Report

2012

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 2012," Audit Control No. ED-OIG/A11M0003, Reporting Metric No. 1, Continuous Monitoring Management, hereafter referred to as FISMA Report.

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

Yes

Comments: No exceptions noted.

1.1.2 Documented strategy and plans for continuous monitoring (NIST 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 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 POA&M additions and updates with the frequency defined in the strategy and/or plans (NIST 800-53, NIST 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

For Official Use Only

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.
"Education Central Automated Processing System (EDCAPS) Information Security Audit," Audit Control No. ED-OIG/A11M0002, hereafter referred to as EDCAPS Report.

2.1.1 Documented policies and procedures for configuration management

Yes

Comments: No exceptions noted.

2.1.2 Standard baseline configurations defined

No

Comments: EDCAPS Report: Finding No. 6, The Department Has Not Implemented a Security Configuration Baseline.

2.1.3 Assessing for compliance with baseline configurations

No

Comments: EDCAPS Report: Finding No. 6, The Department Has Not Implemented a Security Configuration Baseline.

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, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented

Yes

Comments: No exceptions noted.

2.1.6 Documented proposed or actual changes to hardware and software configurations

No

Comments: EDCAPS Report: Finding No. 3, EDCAPS Security Configuration Management Controls Need Improvement.
EDCAPS Report: Finding No. 5, Configuration Management Database Is Not Properly Maintained.

For Official Use Only

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 2a. Patch Management Program Needs Improvement.
EDCAPS Report: Finding No. 2, Patch Management Needed Improvement.

2.1.8 Software assessing (scanning) capabilities are fully implemented (NIST 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 800-53: CM-4, CM-6, RA-5, SI-2)

No

Comments: EDCAPS Report: Finding No. 2, Patch Management Needed Improvement.

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

No

Comments: FISMA Report: Reporting Metric No. 2, Configuration Management, Issue 2a. Patch Management Program Needs Improvement.
EDCAPS Report: Finding No. 2, Patch Management Needed Improvement

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 comments below for exceptions noted

Comments: FISMA Report: Reporting Metric No. 2, Configuration Management, Issue 2b. Access Switch Port Security Needs Improvement.
EDCAPS Report: Finding No. 7, Separation of Duties Needed for G5 Application Users

For Official Use Only

Section 3: Identity and Access Management

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

Yes

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

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

No

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

3.1.2 Identifies all users, including federal employees, contractors, and others who access Organization systems (NIST 800-53, AC-2)

Yes

Comments: No exception noted.

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

Yes

Comments: No exception noted.

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

Yes

Comments: No exception noted.

3.1.5 Organization has adequately 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 exception noted.

3.1.6 Ensures that the users are granted access based on needs and separation of duties principles

Yes

Comments: No exception noted.

For Official Use Only

Section 3: Identity and Access Management

3.1.7 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)

No

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

3.1.8 Identifies all User and Non-User Accounts (refers to user accounts that are on a system. Examples of non-user accounts are accounts such as an IP that is set up for printing. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes that are not associated with a single user or a specific group of users)

Yes

Comments: No exception noted.

3.1.9 Ensures that accounts are terminated or deactivated once access is no longer required

Yes

Comments: No exception noted.

3.1.10 Identifies and controls use of shared accounts

Yes

Comments: No exception 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.

Not used.

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.
EDCAPS Report: Finding No. 4, Keylogger Incident Reporting for G5 Needs Improvement.

For Official Use Only

Section 4: Incident Response and Reporting

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

No

Comments: EDCAPS Report: Finding No. 4, Keylogger Incident Reporting for G5 Needs Improvement.

4.1.2 Comprehensive analysis, validation and documentation of incidents

No

Comments: FISMA Report: Reporting Metric No. 4, Incident Response and Reporting.
EDCAPS Report: Finding No. 4, Keylogger Incident Reporting for G5 Needs Improvement.

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

Yes

Comments: No exceptions noted.

4.1.4 When applicable, reports to law enforcement within established timeframes (SP 800-86)

Yes

Comments: No exceptions noted.

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

No

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

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

Yes

Comments: No exceptions noted.

4.1.7 Is capable of correlating incidents

Yes

Comments: No exceptions noted.

For Official Use Only

Section 4: Incident Response and Reporting

4.1.8 There is sufficient incident monitoring and detection coverage in accordance with government policies (NIST 800-53, 800-61, and OMB M-07-16, M-06-19)

No

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

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

Not used

Section 5: Risk Management

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

Yes

Comments: FISMA Report: Reporting Metric No. 5, Risk Management.
EDCAPS Report: Finding No. 1, The Risk Management Framework Needs Improvement.

5.1.1 Documented and centrally accessible 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.

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 800-37, Rev.1

Yes

Comments: No exceptions noted.

For Official Use Only

Section 5: Risk Management

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

No

Comments: FISMA Report: Reporting Metric No. 5, Risk Management, Issue 5a. Risk Management Program is Not Fully Implemented.

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

No

Comments: EDCAPS Report: Finding No. 1, The Risk Management Framework Needs Improvement.

5.1.5 Categorizes information systems in accordance with government policies

Yes

Comments: No exceptions noted.

5.1.6 Selects an appropriately tailored set of baseline security controls

Yes

Comments: No exceptions noted.

5.1.7 Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation

Yes

Comments: No exceptions noted.

5.1.8 Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system

No

Comments: FISMA Report: Reporting Metric No. 5, Risk Management, Issue 5b. System Authorization Process Needs Improvement.
EDCAPS Report: Finding No. 1, The Risk Management Framework Needs Improvement.

For Official Use Only

Section 5: Risk Management

5.1.9 Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable

No

Comments: FISMA Report: Reporting Metric No. 5, Risk Management, Issue 5b. System Authorization Process Needs Improvement.
EDCAPS Report: Finding No. 1, The Risk Management Framework Needs Improvement.

5.1.10 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

No

Comments: FISMA Report: Reporting Metric No. 5, Risk Management, Issue 5b. System Authorization Process Needs Improvement.
EDCAPS Report: Finding No. 1, The Risk Management Framework Needs Improvement.

5.1.11 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.

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

Yes

Comments: No exceptions noted.

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

Yes

Comments: No exceptions noted.

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

No

Comments: FISMA Report: Reporting Metric No. 5, Risk Management, Issue 5b. System Authorization Process Needs Improvement.

For Official Use Only

Section 5: Risk Management

5.1.15 Security authorization package contains Accreditation boundaries for Organization information systems defined in accordance with government policies.

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 800-53: AT-1)

No

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

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

Yes

Comments: No exceptions noted.

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

Yes

Comments: No exceptions noted.

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

Yes

Comments: No exceptions noted.

For Official Use Only

Section 6: Security Training

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 (SP 800-50, SP 800-53).

Yes

Comments: No exceptions noted.

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

Not used.

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

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

Yes

Comments: FISMA Report: Reporting Metric No. 7, Plan of Action and Milestones.

7.1.1 Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation

No

Comments: FISMA Report: Reporting Metric No. 7, Plan of Action and Milestones.

7.1.2 Tracks, prioritizes and remediates weaknesses

Yes

Comments: No exceptions noted.

7.1.3 Ensures remediation plans are effective for correcting weaknesses

Yes

Comments: No exceptions noted.

For Official Use Only

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

7.1.4 Establishes and adheres to milestone remediation dates

Yes

Comments: No exceptions noted.

7.1.5 Ensures resources are provided for correcting weaknesses

Yes

Comments: No exceptions noted.

7.1.6 POA&Ms include security weaknesses discovered during assessments of security controls and requiring remediation. (Do not need to include security weakness due to a Risk Based Decision to not implement a security control) (OMB M-04-25)

Yes

Comments: No exceptions noted.

7.1.7 Costs associated with remediating weaknesses are identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25)

Yes

Comments: No exceptions noted.

7.1.8 Program officials and contractors 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, and OMB M-04-25)

Yes

Comments: No exceptions noted.

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

Not used.

Section 8: Remote Access Management

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

Yes

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

For Official Use Only

Section 8: Remote Access Management

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

Yes

Comments: No exceptions noted.

8.1.2 Protects against unauthorized connections or subversion of authorized connections.

Yes

Comments: No exceptions noted.

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

Yes

Comments: No exceptions noted.

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

No

Comments: FISMA Report: Reporting Metric No. 8, Remote Access Management, Issue 8a. Remote Access Policy Needs Improvement.

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

No

Comments: FISMA Report: Reporting Metric No. 8, Remote Access Management, Issue 8c. Two-Factor Authentication Exemption Process Needs Improvement.
FISMA Report: Reporting Metric No. 8, Remote Access Management, Issue 8d. Two-Factor Authentication Not Fully Implemented.

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 execptions noted.

For Official Use Only

Section 8: Remote Access Management

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

No

Comments: FISMA Report: Reporting Metric No. 8, Remote Access Management, Issue 8b. FirePass and Citrix Did Not Time-Out After 30 Minutes of Inactivity.

8.1.9 Lost or stolen devices are disabled and appropriately reported (NIST 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 800-53, PL-4)

Yes

Comments: No exceptions noted.

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

Yes

Comments: No exceptions noted.

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

See comments below for exceptions noted.

Comments: FISMA Report: Reporting Metric No. 8, Remote Access Management, Issue 8e. Citrix Inventory Process Needs Improvement.
FISMA Report: Reporting Metric No. 8, Remote Access Management, Issue 8f. Configuration of Non-Government Furnished Equipment Process Needs Improvement.

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.

For Official Use Only

Section 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 800-53: CP-1)

Yes

Comments: No exceptions noted.

9.1.2 The Organization has performed an overall Business Impact Analysis (BIA) (NIST SP 800-34)

No

Comments: FISMA Report: Reporting Metric No. 9, Contingency Planning, Issue 9d. The Business Impact Analysis Process Needs Improvement.

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.
FISMA Report: Reporting Metric No. 9, Contingency Planning, Issue 9e. Contingency Plans Not Documented.

9.1.4 Testing of system specific contingency plans

No

Comments: FISMA Report: Reporting Metric No. 9, Contingency Planning, Issue 9b. Contingency Plan Testing Process Needs Improvement.

9.1.5 The documented business continuity and disaster recovery plans are in place and can be implemented when necessary (FCD1, NIST SP 800-34)

No

Comments: FISMA Report: Reporting Metric No. 9, Contingency Planning, Issue 9c. Principal Offices' Business Continuity Plans Need To Be Updated.

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

Yes

Comments: No exceptions noted.

For Official Use Only

Section 9: Contingency Planning

9.1.7 Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans

No

Comments: FISMA Report: Reporting Metric No. 9, Contingency Planning, Issue 9f. Disaster Recovery Testing Process Needs Improvement.

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

Yes

Comments: No exceptions noted.

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

Yes

Comments: No exceptions noted.

9.1.10 Alternate processing sites are 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 consider 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.

For Official Use Only

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 public cloud

Yes

Comments: No exceptions noted.

10.1.2 The Organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with federal and Organization guidelines

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 public cloud

Yes

Comments: No exceptions noted.

10.1.4 The inventory identifies interfaces between these systems and Organization-operated systems (NIST 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.

For Official Use Only

Section 10: Contractor Systems

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

No

Comments:

FISMA Report: Reporting Metric No. 5- Risk Management, Issue 5b. System Authorization Process Needs Improvement (Modified Repeat Finding).
FISMA Report: Reporting Metric No. 9, Contingency Planning, Issue 9a. Contingency Plans Not Complete.
FISMA Report: Reporting Metric No. 9, Contingency Planning, Issue 9b. Contingency Plan Testing Process Needs Improvement.
FISMA Report: Reporting Metric No. 9, Contingency Planning, Issue 9d. The Business Impact Analysis Process Needs Improvement.
FISMA Report: Reporting Metric No. 9, Contingency Planning, Issue 9e. Contingency Plans Not Documented.
FISMA Report: Reporting Metric No. 9, Contingency Planning, Issue 9f. Disaster Recovery Testing Process Needs Improvement.

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

Not used.

Section 11: Security Capital Planning

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

Yes

Comments: 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.

For Official Use Only

Section 11: Security Capital Planning

11.1.3 Establishes a discrete line item for information security in organizational programming and documentation (NIST 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 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.

For Official Use Only

Enclosure 2: Criteria

"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

FISM 12-02, "FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management", February 15, 2012

OMBM-06-20, "FY 2006 Reporting Instructions for the Federal Information Security Management Act (FISMA) and Agency Privacy Management," July 17, 2006

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

OMB Circular A-11, "Preparation, Submission and Execution of the Budget," August 2011, Section 53—Information Technology and E-Government and Section 300—Planning, Budgeting, Acquisition, and Management of Capital Assets

OMB, "Capital Programming Guide," August 2011

OMB Circular A-123, "Management's Responsibility for Internal Control," December 21, 2004

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

Federal Information Processing Standards (FIPS)-PUB 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004

FIPS-PUB 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006

FIPS-PUB 201-1, "Personal Identity Verification for Federal Employees and Contractors," March 2006

Federal Register Vol. 69, No. 113, United States Office of Personnel Management, 5 CFR 930, "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 Info Systems & Organizations," August 2009

NIST 800-61, Revision 1, "Computer Security Handling Guide," March 2008

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

NIST SP 800-114, "User's Guide to Securing External Devices for Telework and Remote Access," November 2007

NIST SP 800-123, "Guide to General Server Security," July 2008

NIST SP 800-128, "Guide for Security-Focused Configuration Management Information Systems," August 2011

Dell End User Computing Workstation Patch and Configuration Management Process

Federal Student Aid Keylogger Incident Response Standard Operating Procedures, April 2011

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

OCIO -05, "Handbook for Information Technology Security Certification & Accreditation Procedures," March 31, 2006

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

OM 5-102, "Continuity Program," April 27, 2009

MEMORANDUM

DATE: October 19, 2012

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

FROM: Danny A. Harris, Ph.D.
Chief Information Officer
Office of the Chief Information Officer

SUBJECT: Audit of the U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2012, Control Number Audit ED-OIG/A11M0003 Draft Audit Report

Thank you for the opportunity to address the recommendations in the Office of Inspector General's (OIG) draft audit report, regarding the U.S. Department of Education's compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2012, Control Number Audit ED-OIG/A11M0003. The Office of the Chief Information Officer (OCIO) sincerely appreciates the diligence and expertise provided by OIG in conducting this extensive work. The draft audit report underscores the need to ensure that corrective actions are addressed to resolve the noted issues with several of the Reporting Metrics. OCIO will work closely with OIG to manage the response activities appropriately.

At the outset, we note that of the eleven (11) controls audited by OIG, we placed increased emphasis on our Continuous Monitoring program and our Security Capital Planning activities (OIG found that these specific controls were in compliance with existing requirements in 2012.) We believe this emphasis was an appropriate and prudent response for maximizing the overall effect of our efforts to improve the security of Department's information and IT systems, given available resourcing for our IT security and FISMA compliance programs. As we move forward, we plan to leverage improvements in these control areas to justify increased investment in our IT security and FISMA compliance programs in order to align such investments more closely with key metrics published by Gartner and others.

The following OCIO responses address each recommendation:

REPORTING METRIC NO. 1 – Continuous Monitoring Management

The OIG found the Department complied with this reporting metric.

REPORTING METRIC NO. 2 - Configuration Management (Repeat Finding)

OIG Conclusion 2a. – Patch Management Program Needs Improvement (Repeat Finding).

OIG Recommendation 2a. - Corrective actions to address this recommendation contained in the FY2011 FISMA report are still outstanding. OCIO to "Develop, approve, and implement an enterprise-wide patch management policy that complies with OMB, NIST, and other applicable Federal guidelines. Circulate and distribute the final approved patch management policy to all principal offices and contractors for consistent implementation." See http://www2.ed.gov/about/offices/list/oig/auditreports/fy2012/a11l0003.pdf, page 15 of 79.

Management Response: OCIO concurs with this recommendation. The Department has undertaken a complete revision of the "Vulnerability and Patch Management Guidance" and processes to ensure compliance with OMB, NIST, and other applicable Federal guidelines. The new patch management policy will be completed and distributed to all relevant stakeholders by May 15, 2013.

OIG Conclusion 2b. – Access Switch Port Security Needs Improvement (Repeat Finding).

OIG Recommendation 2b. - Corrective actions to address this recommendation contained in the FY2011 FISMA report are still outstanding. OCIO to "Require the contractor to establish access switch port security in accordance with NIST and the DISA Network Security Checklist on all switch ports within the enterprise, except network uplinks. Require the contractor to shut down or disable unassigned/unused switch port connections throughout the enterprise." See http://www2.ed.gov/about/offices/list/oig/auditreports/fy2012/a11l0003.pdf, page 15 of 79.

Management Response: OCIO concurs with this recommendation. OCIO Information Technology Services (ITS), for the EDUCATE network, and Information Assurance Services (IAS) will work with the appropriate vendors to develop and implement security configuration baselines for all Department devices, including switches, which will incorporate best practices from NIST and Defense Information Systems Agency Network Security Checklists, and other related guidance. The Department Chief Information Security Officer (CISO) will issue a memorandum, by December 01, 2012, to the Director of ITS, to instruct the support contractor to: establish access switch port security in accordance with NIST and the Defense Information Systems Agency Network Security Checklist on all switch ports within the enterprise, except network uplinks; and, shut down or disable unassigned/unused switch port connections. The target completion date to shut down or disable unassigned/unused switch port connections throughout the enterprise is August 15, 2013.

REPORTING METRIC NO. 3 – Identity and Access Management (Repeat Finding)

OIG Conclusion - Corrective actions to address this recommendation contained in the FY2011 FISMA report are still outstanding. "We recommend that the OCIO establish and implement policies and procedures 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 applicable regulations, guidance, and standards established by OMB and NIST." See http://www2.ed.gov/about/offices/list/oig/auditreports/fy2012/a11l0003.pdf, page 25 of 79.

Management Response: OCIO concurs with this recommendation. In September 2012, IAS awarded a Continuous Monitoring task order to implement tools to identify and monitor devices on the network. Initial Operational Capability (IOC) is scheduled for the end of 4th quarter FY13. In addition, the target completion date to implement a Network Admission Control (NAC) solution that will allow the Department to (1) identify all devices that are attached to the network; (2) distinguish the devices from users; and (3) authenticate devices that are connected to the network consistent with FISMA, OMB, and NIST guidance is September 15, 2013.

REPORTING METRIC NO. 4 - Incident Response and Reporting

OIG Recommendation 4.1 – Review logs for the remaining 606 and 72 compromised privileged accounts from calendar year 2011 and 2012, respectively.

Management Response: OCIO concurs with this recommendation: FSA has awarded a contract task to its independent security review team to complete log reviews for all privileged user compromises identified through analysis of files provided from US-CERT. The target completion date to review logs for the remaining 606 and 72 compromised privileged accounts from calendar year 2011 and 2012 is May 15, 2013.

OIG Recommendation 4.2 – Enforce the requirement for ISSOs to perform a log review of all compromised privileged accounts to ensure incidents are properly remediated in accordance with "FSA Keylogger Incident Response Standard Operating Procedures".

Management Response: OCIO partially-concurs with this recommendation. Although FSA believes this is one approach that could be used, FSA has implemented an alternative approach that they believe is more effective. FSA has awarded a contract task to its independent security review team to complete log reviews for all privileged user compromises identified through analysis of files provided from US-CERT. OCIO has agreed to convert the "FSA Keylogger Incident Response Standard Operating Procedures" into a Department-wide process, and update it with the approach for centralized support. By May 15, 2013, this approach will systemically improve the Department's management of keylogger incidents and enforce the requirement for ISSOs to perform a log review of all compromised accounts to ensure incidents are properly remediated in accordance with "FSA Keylogger Incident Response Standard Operating Procedures".

OIG Recommendation 4.3 – Ensure that ISSOs receive proper training so they can properly review system event audit logs for compromised privileged accounts.

Management Response: OCIO partially-concurs with this recommendation. Although FSA believes this is one approach that could be used, FSA has implemented an alternative approach that they believe is more effective. FSA has awarded a contract task to its independent security review team to complete log reviews for all privileged user compromises identified through analysis of files provided from US-CERT. This approach was discussed with the OIG and the OIG agreed with this approach. Although, FSA's approach to satisfy this finding and recommendation differ from the OIG's recommendation, FSA agrees with OIG that ISSOs should be trained to complete the log reviews as recommended and will provide training during its monthly ISSO meetings to ensure ISSOs complete this activity. The training will be completed by September 15, 2013.

OIG Recommendation 4.4 – Review and amend or modify all contracts (as applicable) to have audit logs provided to FSA and require ISSOs to perform log reviews of compromised privileged accounts.

Management Response: OCIO partially-concurs with this recommendation. FSA concurs that a review should be made of all contracts to determine contract responsibility for log submissions. Once gaps are identified, FSA plans to work with its Business Units to modify or amend contracts. Contract expiration dates and cost will be used to determine best alternatives. FSA does not concur with the recommendation to require ISSOs perform log reviews. Although FSA believes this is one approach that could be used, FSA has implemented an alternative approach that they believe is more effective. FSA has awarded a contract task to its independent security review team to complete log reviews for all privileged user compromises identified through analysis of files provided from US-CERT. This approach was discussed with the OIG, and the OIG agreed with this approach. The contractors work will be reviewed to a) to assess fidelity of implementation and b) to assess implications of log reviews by September 15, 2013.

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 OMB and NIST." See http://www2.ed.gov/about/offices/list/oig/auditreports/fy2012/a11l0003.pdf, page 10 of 79.

Management Response: OCIO partially-concurs with this recommendation. While OCIO has not updated OCIO-01 or OCIO-05 to include Risk Management, OCIO published "Information System Security Authorization Guidance," on June 15, 2011. The "Information System Security

Authorization Guidance" includes a comprehensive governance structure and organization-wide risk management strategy that includes the techniques and methodologies that the Department will employ to assess information system related risk to preserve availability, confidentiality, and integrity. OCIO will complete a comprehensive risk management implementation plan including policies and procedures by 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 all system authorization documentation is readily available and complies with Federal and Department standards and guidance, and take immediate action to resolve the deficiencies identified in Issue 1b (a list of systems and applicable documentation was provided to the OCIO). 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), and take immediate action to properly authorize the systems in Issue 1b. A list of systems was provided to the OCIO. Develop controls to ensure timely re-authorizations for systems, avoiding gaps in ATO coverage. Update the OCIO-05 and OCIO-01 handbooks to be in compliance with OMB and NIST guidance with respect to risk management and interim ATOs." See http://www2.ed.gov/about/offices/list/oig/auditreports/fy2012/a11l0003.pdf, page 11 of 79.

Management Response: OCIO partially-concurs with this recommendation. "Information System Security Authorization Guidance", published June 15, 2011, is consistent with NIST SP 800-37, and provides documentation of a common controls document. As noted above, OCIO will complete a comprehensive risk management plan by September 30, 2013 to help improve the security authorization process. In addition, we would like to note that the following actions are in progress:

- OCIO awarded a new contract in FY12 to provide additional support for the implementation of the risk management framework.
- In order to develop controls to ensure timely re-authorizations for systems, avoiding gaps in ATO coverage, OCIO is working with ISSOs and system owners to ensure OVMS accurately reports ATO approval dates by March 2013, and to ensure completeness of Certification and Accreditation (C&A) packages through one-on-one sessions with principal office ISSOs and system owners, and by increasing the frequency of ISSO meetings from every other month to monthly.

OCIO believes these activities significantly improve the Security Authorization Process.

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

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. Revise the IT security awareness and training program policies and procedures to require that the training in Recommendation 4.1 above be completed prior to access to the Department's network or any Departmental information systems." See http://www2.ed.gov/about/offices/list/oig/auditreports/fy2012/a11l0003.pdf, page 18 of 79.

Management Response: OCIO has completed action to satisfy this recommendation (July 2012). OCIO, in conjunction with its security awareness and training support contractor, developed a "New Employee Cyber Security and Privacy Orientation" course that is provided as part of the Department's Corporate Onboarding Process, EDStart on-line, and is posted on the ED.gov website (http://www2.ed.gov/about/offices/list/om/onboard/first-day.html). All new departmental employees are required to complete this course in advance of reporting onboard, and to provide proof of course completion when they report for employee orientation. In addition, we've also updated and improved our annual security awareness training material, consolidating information security with privacy training. We also continue to hold security awareness training activities and events during DHS' October Cybersecurity Awareness Month observance annually.

REPORTING METRIC NO. 7 – Plan of Action and Milestones

OIG Recommendation 7.1 - We recommend that the OCIO update the current POA&M procedures to include the processes and procedures for informing management when POA&Ms are not met.

Management Response: OCIO concurs with this recommendation. The Department will review and update its POA&M procedures. The new POA&M procedures will be submitted for stakeholder review by March 31, 2013 (30 day review period) with a target completion date of May 15, 2013.

REPORTING METRIC NO. 8 – Remote Access Management

OIG Recommendation 8.1 – Validate the changes to the FirePass inactivity settings to ensure sessions are timing out after 30 minutes of inactivity.

Management Response: OCIO concurs with this recommendation. OCIO will validate that FirePass inactivity settings are set to time out sessions after 30 minutes of inactivity by December 31, 2012.

OIG Recommendation 8.2 – Distribute dual-authentication tokens to all guaranty agency users and all other external business partners with privileged accounts in order to comply with OMB and NIST mandates.

Management Response: OCIO concurs with this recommendation. FSA has already factored guaranty agency distribution into the overall plan that FSA has been actively moving forward on since January 2012. As referenced in FSA's response to this finding, please see the comment below:

Comment: The 300 two factor tokens mentioned in the OIG report are part of an international two-factor deployment effort led by FSA that focused on high priority risks. Additionally, to date, nearly 60,000 tokens have been deployed to users in approximately 35 countries since January 2012. The project based its deployment strategy on a risk-based model that started with deployment for all Department employees, followed by foreign nation institutions participating in the Title IV program. United States based deployment started in Spring 2012 and is expected to complete by Spring 2013. We also note that of this writing, nearly 30,000 users have registered and are in full use of the two-factor technology. Of the 6,500 US based institutions who have received tokens to date, 29,246 have had all user accounts set to "Required." The transition of residual institutions to "Required" will be completed by the Spring 2013 date.

OIG Recommendation 8.3 – Configure webmail to require dual authentication as mandated by OMB-06-16 and OMB-07-16, or allow email to be accessible only via FirePass sessions that use dual authentication.

Management Response: OCIO concurs with this recommendation. Outlook Web Access (OWA) is the technology currently utilized by the Department to deliver web mail services to the user base. Although it is possible to do two-factor authentication with OWA, OCIO is currently working with Dell Systems to determine the best way to implement this solution utilizing the existing PIV Card / VeriSign Token. We expect to be able to have a plan in place by the end of 3rd quarter FY 2013. Based upon the plan, OCIO management will determine if we will implement the aforementioned approach, or move to a FirePass only solution. The final solution will be implemented by December 31, 2013.

OIG Recommendation 8.4 – Develop written policies and procedures to define the dual-authentication exemption requirements and process.

Management Response: OCIO non-concurs with this recommendation. Remote access through Firepass requires dual authentication and there are no exemptions allowed. As such, no policy or procedure is required. If determined an exemption is applicable and/or appropriate, OCIO will develop the corresponding policies, procedures, and processes for managing.

OIG Recommendation 8.5 – Formally document the Department's position to accept the risk to allow single-factor authentication for those individuals that meet the exemption requirements.

Management Response: OCIO non-concurs with this recommendation. Remote access through Firepass requires dual authentication and there are no exemptions allowed. As such, no policy or procedure is required. If determined an exemption is applicable and/or appropriate, OCIO will develop the corresponding policies, procedures, and processes for managing.

OIG Recommendation 8.6 – Update the telework policy 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 policy requirements and coordinate with stakeholders on alternatives for performing validation of security of non-GFE devices used to connect to the Department's network remotely. OCIO will complete this action by no later than September 30, 2013.

OIG Recommendation 8.7 – Ensure that a complete inventory is documented and maintained that accurately accounts for all Citrix servers used in the production environment, and ensure that changes are made in a timely manner to accurately represent the current overall infrastructure.

Management Response: OCIO concurs with this recommendation. OCIO is taking steps to ensure that the Citrix servers are documented in the System Security Plans (SSP). Dell Services is required to provide quarterly, a deliverable of each EDUCATE SSP. The latest inventory accounts for all Citrix servers and been included in the EDUCATE SSPs approved in September 2012.

OIG Recommendation 8.8 – Identify and maintain tracking of teleworkers who use non-GFEs to connect to the network remotely and ensure those devices have been configured to the standards set forth in the telework requirements.

Management Response: OCIO partially-concurs with this recommendation. In response to identifying and maintaining tracking of teleworkers who use non-GFEs to connect to the network remotely, departmental telework policy (Flexiplace Work Agreement) requires employees provide asset information on the information technology equipment they will be using to conduct their telework activities. Employees are also notified of the expectations for applying approved safeguards to protect Government/agency records from unauthorized disclosure or damage.

The issue of the Department being able to ensure that non-GFE devices have been configured to standards set forth in the telework requirements has proven to be problematic. The Department's Office of General Counsel (OGC) and the Office of Management (OM) have been party to past discussions regarding the legality of the Department's being able to treat non-GFE as if it were GFE. To declare that only GFE devices may attach and work on the Department's networks and systems would necessitate an enormous outlay of funding to purchase GFE for anyone wishing to telework. We currently feel this solution is not feasible.

The OCIO has been investigating endpoint inspection capabilities, as a means of checking devices for compliance with GFE standards. Whether a viable solution is forthcoming is not clear at this point in time, and we will continue to keep OIG apprised of our progress on this issue.

REPORTING METRIC NO. 9 – Contingency Planning

OIG Recommendation 9.1 – Review and update information system contingency plans for the 14 systems that have elements missing (list provided to OCIO) to ensure that all the contingency planning elements are included as required by NIST guidance.

Management Response: OCIO concurs with this recommendation. OCIO will coordinate with ISSOs and system owners for the 14 identified systems, to create plans of actions and milestones for the review and update of information system contingency plans, as appropriate, by December 31, 2012.

OIG Recommendation 9.2 – Perform and document information system contingency plan test results for the National Household Education Survey System and Higher Education Programs Field Reader System as required by NIST guidelines and Departmental procedures.

Management Response: OCIO concurs with this recommendation. OCIO will coordinate with ISSOs and system owners for the National Household Education Survey System and Higher Education Programs Field Reader System to develop a plan for contingency plan testing by February 28, 2013.

OIG Recommendation 9.3 – Ensure ISSOs or system owners perform annual contingency plan testing and document test results as required by NIST guidelines and Departmental procedures.

Management Response: OCIO concurs with this recommendation. The current "Information System Security Authorization Guidance", which was issued June 2011, specifically requires annual contingency plan testing. OCIO will leverage reporting from the Operational Vulnerability Management Solution (OVMS) and monthly ISSOs meetings to ensure ISSOs and system owners are aware of the requirement to perform annual contingency plan testing and to document their test results.

OIG Recommendation 9.4 – Develop and maintain individual information system contingency plans and disaster recovery plans for EDMASS, EDNIS, and EDSOC.

Management Response: OCIO partially-concurs with this recommendation. EDMASS and EDNIS were combined into a single security boundary in FY12 called Infrastructure, which has a contingency plan and disaster recovery plan separate from the other EDUCATE security boundaries. The contingency and disaster recovery plans for each security boundary will be uploaded in OVMS by no later than December 31, 2012.

OIG Recommendation 9.5 – Update Departmental policies and procedures to define the requirement for the consolidation of general support systems and major application contingency plans and disaster recovery plans as part of contingency planning procedures.

Management Response: OCIO partially-concurs with this recommendation. The current "Information System Security Authorization Guidance", which was issued June 2011,

specifically refers to a contingency plan as including "procedures for the assessment and recovery of a system following a system disruption" which covers both contingency planning and disaster recovery.

OIG Recommendation 9.6 – Ensure ISSOs or system owners perform and document a BIA as part of contingency planning for all systems in accordance with NIST guidelines and Departmental procedures.

Management Response: OCIO concurs with this recommendation. OCIO will leverage reporting from OVMS and monthly ISSOs meetings, to ensure ISSOs and system owners are aware of the requirement to perform and document a BIA as part of contingency planning. This will commence immediately and continue as an ongoing activity.

OIG Recommendation 9.7 – Develop Citrix recovery procedures to use during disaster recovery testing, and document the results of test performed.

Management Response: OCIO concurs with this recommendation. OCIO will develop Disaster Recovery Procedures and incorporate them into the Infrastructure GSS Information System Contingency Plan (ISCP) and its included Disaster Recovery Plan. OCIO will document the results of the test to be performed in May 2013 in the OVMS database.

OIG Recommendation 9.8 – Require principal offices to update the BCPs for the six systems that have elements missing (list provided to OCIO) to ensure that all the required BCP elements are included in accordance with the Department's BCP template.

Management Response: OCIO concurs with this recommendation. OCIO will require principal offices, for the six systems identified, to submit a plan of action and milestones for updating the BCPs by December 31, 2012.

OIG Recommendation 9.9 – Review the remaining principal offices' BCPs for completeness and accuracy to ensure they are in accordance with the Department's BCP template.

Management Response: OCIO concurs with this recommendation. OCIO will leverage reporting from OVMS and monthly ISSOs meetings, to ensure ISSOs and system owners review BCPs for completeness and accuracy, in accordance with the Department's BCP template. This will be an ongoing activity. This will commence immediately and continue as an ongoing activity.

REPORTING METRIC NO. 10 – Contractor Systems

OIG Recommendation – Review the remaining principal offices' BCPs for completeness and accuracy to ensure they are in accordance with the Department's BCP template.

Management Response: OCIO concurs with this recommendation. OCIO will leverage reporting from OVMS and monthly ISSOs meetings, to ensure ISSOs and system owners review

BCPs for their contractor systems for completeness and accuracy, in accordance with the Department's BCP template. This will commence immediately and continue as an ongoing activity.

REPORTING METRIC NO. 11 – Security Capital Planning

The OIG found the Department complied with this reporting metric.

Thank you for the opportunity to respond to this report. If you have any questions regarding this matter, please contact me at (202) 245-6252 or Danny.Harris@ed.gov.