The U.S. Department of Education's Compliance with the Federal Information Security Management Act for Fiscal Year 2011

FINAL AUDIT REPORT

ED-OIG/A11L0003
October 2011

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

ATO	Authorization to Operate
BCP	Business Contingency Plan
BIA	Business Impact Analysis
CAMS	Case Activity Management System
CAT	Category
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
COCO	Contractor Owned Contractor Operated
COOP	Continuity of Operation Plans
CPS	Central Processing System
CSA	Continuous Security Authorization
CSAM	Cyber Security Assessment and Management
DAA	Designated Approving Authority
Department	U.S. Department of Education
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DMCS	Debt Management and Collection System
DRP	Disaster Recovery Plan
EDCAPS	Department of Education's Central Automated Processing System
EDCIS	EDUCATE Data Center Information System
EDMASS	EDUCATE Mass Storage System
EDNIS	Education Network Infrastructure System
EDSOC	EDUCATE Security Operations Center
EDSTAR	Education's Security Tracking and Reporting System
EDUCATE	Education Department Utility for Communications, Applications, and Technology Environment
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FSA	Federal Student Aid
FY	Fiscal Year
GAO	Government Accountability Office
GFE	Government Furnished Equipment
GISRA	Government Information Security Reform Act
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
IG	Inspector General
IP	Internet Protocol
IPAR	Investigative Program Advisory Report
IRM	Information Resources Management
ISA	Interconnection Security Agreement
IT	Information Technology
LAN	Local Area Network
Level	FIPS Publication 199 potential impact level
MDF	Main Distribution Frame

MOU	Memorandum of Understanding
MSSP	Managed Security Service Provider
NIST	National Institute of Standards and Technology
NSLDS	National Student Loan Data System
OCO	Office of Communications & Outreach
OCR	Office for Civil Rights
OCIO	Office of Chief Information Officer
OIG	Office of Inspector General
OM	Office of Management
OMB	Office of Management and Budget
OPE	Office of Postsecondary Education
OPEPD	Office of Planning, Evaluation and Policy Development
OPM	Office of Personnel Management
OS	Office of the Secretary
OSERS	Office of Special Education and Rehabilitative Services
OVMS	Operational Vulnerability Management System
Perot Systems	Perot Systems Government Services
PII	Personally Identifiable Information
PIRWG	Planning and Investment Review Working Group
PO	Principal Office
POA&M	Plan of Action and Milestones
RAF	Risk Acceptance Form
SAR	Security Assessment Report
SI	System and Information Integrity
SLA	Service Level Agreement
SMB	Server Message Block
SP	Special Publication
SSH-1	Secure Shell Version 1
SSP	System Security Plan
TFA	Two Factor Authentication
TSP	Telecommunication Service Priority
TFMS	Treasury Financial Management System
US-CERT	U.S. Computer Emergency Response Team
VDC	Virtual Data Center

UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Information Technology Audit Division

October 18, 2011

Memorandum

TO: Danny A. Harris, Ph.D.
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 for Fiscal Year 2011
Control Number ED-OIG/A11L0003

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 2011. An electronic copy has been provided to your Audit Liaison Officer. We received your comments concurring, partially concurring, or not concurring with 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 (AARTS). ED policy requires that you develop a final corrective action plan (CAP) for our review in the automated system within 30 days of the issuance of this report. The CAP should set forth the specific action items, and targeted completion dates, necessary to implement final corrective actions on the findings and recommendations contained in this final audit report.

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

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

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

Enclosure

Cc: Michele Iversen, Director for Information Assurance Services, Office of Chief Information Officer (OCIO)
Phill Loranger, Deputy Director for Information Assurance Services, OCIO
Dana Stanard, Audit Liaison, OCIO
Marge White, Audit Liaison for 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

The Office of Chief Information Officer (OCIO) provides advice and assistance to the Secretary and other senior officials to ensure that information technology (IT) is acquired and information resources are managed in a manner that is consistent with the requirements of the Information Technology Management Reform Act of 1996 and the Federal Information Security Management Act of 2002 (FISMA). The agency's Chief Information Officer (CIO) 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 U.S. Department of Education (Department) operations.

The Department manages a $3 billion total IT investment portfolio, spending $579 million on the IT portfolio for fiscal year (FY) 2011. The Department budgeted $7.5 million for FY 2011 and $9.8 million for FY 2012 on IT security and FISMA compliance costs. As of June 30, 2011, the Department reported an inventory of 162 IT systems.

This report constitutes the Office of Inspector General's (OIG) independent evaluation of the Department's IT security program and practices as required by the FISMA. The OIG's review is based on Office of Management and Budget (OMB)-provided questions for the FY 2011 FISMA review, which are designed to assess the status of the Department's security posture in FY 2011. For the FY 2011 FISMA review, OMB's framework requires us to evaluate processes, policies, and procedures that had already been implemented and documented and were being monitored. 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 2011 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 IT security program and practices comply with the E-Government Act (Public Law 107-347) including Title III, FISMA, and 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]

OMB issued the Inspectors General (IG) metrics, or controls areas, to be assessed for FY 2011 FISMA compliance in June 2011. The 11 controls areas included Risk Management, Configuration Management, Incident Response and Reporting, Security Training, Plan of Actions and Milestones, Remote Access Management, Identity and Access Management, Continuous Monitoring Management, Contingency Planning, Contractor Systems, and Security

[1] For purposes of this audit, enterprise-level security controls are controls that are expected to be implemented department-wide—security training, incident response and reporting, and configuration management—and are not system-specific.

Capital Planning. This FY 2011 FISMA review identified findings in each of the OMB reporting metrics or controls areas. In addition, 5 of the 11 controls areas—Risk Management, Configuration Management, Remote Access Management, Identity and Access Management, and Contingency Planning—contained repeat findings from OIG reports issued during the prior 3 years, FY 2008 through FY 2010.[2] We answered the questions in the OMB metrics template that will be input to the CyberScope FISMA Report as shown in Enclosure 1.

Department systems contain or protect an enormous amount of confidential information (personal records, financial information, and other Personally Identifiable Information [PII]) and perform vital organizational functions. Unauthorized individuals might target the systems by exploitation, but the systems could also be targeted by trusted individuals inside the contractor's organization. Without adequate management, operational, and technical security controls in place, the Department's systems and information are vulnerable to attacks that could lead to a loss of confidentiality caused by unauthorized access to data and to a possible loss of integrity through data modification or limited availability from unauthorized access and excessive use of system resources. Also, there is increased risk that unauthorized activities may occur that reduce the reliability of Department systems and data being maintained, as well as the potential that sensitive data may be released, used, or modified.

We made 18 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 (NIST) requirements. These recommendations supplement those made in other reports issued earlier in the year.

In response to our draft report, the OCIO thanked the OIG for the opportunity to comment on this report and for our continued support of the Department and its critical mission. The OCIO concurred with the findings and recommendations with the exceptions of Finding Issue 6c, Recommendation 2.4, and Recommendation 6.5. Specifically, the OCIO disagreed with Finding Issue 6c that two-factor authentication was not implemented, partially concurred with Recommendation 2.4, and did not concur with Recommendation 6.5. Further, the OCIO disagreed with findings from the issued EDUCATE report and the presentation of repeat findings that listed prior OIG audit report findings in specified controls areas. Additionally, the OCIO stated that the Department has garnered significant benefits from previous years' audits and expects that the recommendations presented in this current audit will further improve the information security program by strengthening the associated management, technical, and operational security controls. The OCIO stated concerns regarding methodology for this audit and we addressed the concerns in the "Audit Results" section as the methodology applies to the audit as a whole. We summarized and responded to specific comments in the "Findings" section of the audit report. We considered the OCIO's comments but did not alter or revise our findings or recommendations. However, issues discussed during the exit conference held on October 6, 2011 resulted in our modification of Recommendation 1.3. The OCIO's response is included as Enclosure 3 to this audit report.

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

BACKGROUND

The E-Government Act (Public Law 107-347), passed by the 107th Congress and signed into law by the President 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, the Federal Information Security Management Act (FISMA), permanently reauthorized the framework established by the Government Information Security Reform Act (GISRA) of 2000, which expired in November 2002. FISMA continued the annual review and reporting requirements introduced in GISRA but 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 responsibility for developing standards and guidelines, including the development of:

- 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 (i.e., 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, and pursuant to its statutory authorities, the Department of Homeland Security (DHS) oversees critical infrastructure protection, operates the United States Computer Emergency Readiness Team (US-CERT), 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 the submission of the annual FISMA report to Congress, for the development and approval of the cybersecurity portions of the President's Budget, and for the traditional OMB budgetary and fiscal oversight of the 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.

FISMA also assigned specific responsibilities to OMB, agency heads, Chief Information Officers (CIO), and Inspectors General (IG). 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:

- periodic risk assessments that consider internal and external threats to the integrity, confidentiality, and availability of systems, and to data supporting critical operations and assets;
- development and implementation of risk-based, cost-effective policies and procedures to provide security protections for the agency's information;
- training that covers security responsibilities for information security personnel and security awareness for agency personnel;
- periodic management testing and evaluation of the effectiveness of security policies, procedures, controls, and techniques;
- processes for identifying and remediating significant security deficiencies;
- procedures for detecting, reporting, and responding to security incidents; and
- annual program reviews by agency officials.

In addition to the responsibilities listed above, FISMA requires each agency to have an annual independent evaluation of its information security program and practices, including control testing and a compliance assessment. The evaluations are to be performed by the agency's IG or an independent evaluator, and the results of these evaluations are to be reported to OMB. Beginning in FY 2009, OMB required Federal agencies to submit FISMA reporting through the OMB web portal, CyberScope.

For FY 2011 FISMA reporting, we judgmentally selected 16 systems for review. Of the 16 systems selected, we included 7 from the judgmental sample performed as part of our FY 2010 review. We selected these systems in order to measure progress from the prior fiscal year. The remaining 9 systems were judgmentally selected based on the system risk level of moderate or high from the Department's principal office (PO) components that managed greater numbers of systems. [3] We reviewed specific aspects of security controls for the sample, including risk management, system authorization, configuration management, and contingency planning.

The U.S. Department of Education (Department) entered into a contract with Perot Systems Government Services (Perot Systems) to provide and manage all IT infrastructure services to the Department under the Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) system. [4] The contract established a Contractor Owned and Contractor Operated (COCO) IT service model for the Department under which Perot Systems provides the total IT platform and infrastructure to support Department employees in meeting the Department's mission. The contract was awarded in September 2007 as a 10-year,

[3] FIPS 199, dated 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, organizational 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 organization operations, organizational assets, or individuals.

[4] Perot Systems was acquired by Dell in September 2009.

performance-based, indefinite delivery/indefinite quantity contract with fixed unit prices. Under the COCO contract, Perot Systems 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 (SLA) 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 (EDCIS), and Case Activity Management System (CAMS), as well as the wide-area and local-area network hardware consisting of network servers, routers, switches, and external firewalls.

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 VDC is considered by the Department to be a general support system and consists of networks, mainframe computers, operating system platforms, and the corresponding operating systems. The VDC is also managed by Perot Systems 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.

AUDIT RESULTS

OMB issued the IG metrics, or controls areas, to be assessed for FY 2011 FISMA compliance in June 2011. The 11 controls areas included Risk Management, Configuration Management, Incident Response and Reporting, Security Training, Plan of Actions and Milestones, Remote Access Management, Identity and Access Management, Continuous Monitoring Management, Contingency Planning, Contractor Systems, and Security Capital Planning.

As part of this year's FISMA review, we incorporated results and findings from two OIG reports, "Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) Information Security Audit," ACN A11L0001, issued September 30, 2011, and Investigative Program Advisory Report (IPAR) "Incident Response and Reporting Procedures," ACN L21L0001, dated June 14, 2011. Additionally, we included applicable results from the United States Government Accountability Office (GAO), Report to the Ranking Member, Committee on Education and the Workforce, House of Representatives, "Department of Education, Improved Oversight and Controls Could Help Education Better Respond to Evolving Priorities," GAO-11-194, issued in February 2011. These three reports contain recommendations to address deficiencies identified in them. The recommendations made by this FY 2011 FISMA review are in addition to those made in the three named reports.

This FY 2011 FISMA review identified findings in each of the OMB reporting metrics or controls areas. Details are provided by controls areas and presented as listed in the OMB metrics, with the exception of Continuous Monitoring that was reported as a subset of Risk Management in Finding No. 1. In addition, 5 of the 11 controls areas—Risk Management, Configuration Management, Remote Access Management, Identity and Access Management, and Contingency Planning—contained repeat findings from OIG reports issued during the prior 3 years, FY 2008 through FY 2010. We answered the questions in the OMB metrics template that will be input to the CyberScope FISMA Report as shown in Enclosure 1.

In response to our draft report, the OCIO thanked the OIG for the opportunity to comment on this report and for our continued support of the Department and its critical mission. The OCIO concurred with the findings and recommendations with the exceptions of Finding Issue 6c, Recommendation 2.4, and Recommendation 6.5. Specifically, the OCIO disagreed with Finding Issue 6c that two-factor authentication was not implemented, partially concurred with Recommendation 2.4, and did not concur with Recommendation 6.5. Further, the OCIO disagreed with findings from the issued EDUCATE report and the presentation of repeat findings that listed prior OIG audit report findings in specified controls areas. Additionally, the OCIO stated that the Department has garnered significant benefits from previous years' audits and expects that the recommendations presented in this current audit will further improve the information security program by strengthening the associated management, technical, and operational security controls. The OCIO stated concerns regarding methodology for this audit and we addressed the concerns below as the methodology applies to the audit as a whole.

Management's General Response to the Report

The results of the FISMA audit clearly indicate that the Department continues to show incremental and credible improvement in meeting the requirements of the FISMA. While the OCIO agrees with many of the findings and recommendations arising from this audit, we believe that the methodology used to conduct this audit limited the OIG's ability to produce a fair and balanced report. Specifically, (1) the timing of the audit did not allow the OIG to acknowledge the Department's final set of achievements for the 2011 fiscal year; (2) throughout the report the OIG references system-specific findings from previously issued OIG reports, but fails to mention that these findings have since been resolved by the Department; and, (3) several recommended actions were already under way at the time of the OIG's review, and, as noted below, some were completed before the first draft review was provided to management.

OIG Response

(1) The timing of the FISMA audit was dictated by OMB reporting requirements and not by the OIG. As described in the Executive Summary and the Background of this report, OMB requires that agency IGs evaluate the CIO's management of IT assets and FISMA compliance for FY 2011, which ends September 30, 2011. (2) We reference prior OIG audit report findings to evidence that the repeat conditions identified are persistent security control deficiencies that have not been addressed enterprise-wide or organization-wide. Although management may have taken corrective actions for individual systems reviewed in prior audits, the central issue remains that deficiencies identified are not corrected organization-wide. Consequently, we continue to identify systemic deficiencies. (3) The OMB IG metrics ask whether the agency has policies and processes in place or procedures implemented in accordance with FISMA, OMB, and NIST. Although we acknowledged proactive steps taken toward FISMA compliance, we answered the OMB questions based on the state of the security control during our audit. We did not include planned management actions that were scheduled for future dates and could not, therefore, be verified by our audit review. Additionally, OMB asked whether procedures were consistently implemented. Procedures that are partially but not fully implemented cannot be measured for consistent implementation by Department personnel.

We summarized and responded to specific comments in the "Findings" section of the audit report. We considered the OCIO's comments but did not alter or revise our findings or recommendations. However, issues discussed during the exit conference held on October 6, 2011 resulted in our modification of Recommendation 1.3. The OCIO's response is included as Enclosure 3 to this audit report.

FINDING NO. 1 -- Risk Management

Issue 1a - The OCIO Needs to Fully Implement the Risk Management Program

The OCIO did not timely implement a risk management program that is consistent with NIST Special Publication (SP) 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems," dated February 2010. Specifically, the Department needs to enhance its continuous system authorization and continuous monitoring procedures to ensure that security controls are monitored on an ongoing basis. NIST SP 800-37, Revision 1 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 highly diverse environments of complex and sophisticated cyber threats, ever-increasing system vulnerabilities, and rapidly changing missions. Current Department policies and procedures for continuously monitoring security controls are based on NIST SP 800-37 guidance published in May 2004. OMB policy states that agencies are expected to be in compliance with NIST standards and guidelines within 1 year of the publication date unless otherwise directed by OMB. [5] The OCIO did not update and implement the risk management policies and procedures for continuous system authorization and continuous monitoring to meet the 1-year compliance date for implementing revisions to NIST publications and guidelines. As a result, personnel do not have current Department guidance that is consistent with NIST guidance on the risk management framework.

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

- A Chief Information System Security Officer (CISO) position was established to oversee the Information Assurance (IA) program and provide strategic guidance for information assurance, cyber security, and risk management.
- An IA Board of Directors was established in December 2010 to guide and direct the agency-wide risk management strategy, provide risk mitigation guidance, and establish risk tolerance for the Department.
- The CISO initiated a Department-wide Security Architecture Working Group to assess enterprise security capabilities.

Issue 1b - The OCIO Needs to Improve the System Authorization Process

The Department's system authorization process needs improvement. Our review identified deficiencies in system security plans (SSPs), authorization to operate (ATO) documents, memoranda of understanding (MOU), security assessment reports (SAR), and expired system authorizations (formerly called certification and accreditation). More specifically, for the 16 systems judgmentally selected to review:

- 1 of 16 systems, the Federal Information Processing Standards (FIPS) 199 level in the system security plan did not match the FIPS 199 level in the FISMA FY 2011 Inventory (as of June 30, 2011) and MOUs and interconnection security agreements (ISAs) were not found for all system interconnections.
- 1 of 16 systems, the SAR was outside of the system authorization period.
- 1 of 16 systems, the SAR and related Plan of Action and Milestones (POA&M) were not found.
- 4 of 16 systems, SSPs were not reviewed on an annual basis.

[5] OMB Memorandum M-10-15, "FY 2010 Reporting Instructions for the Federal Information Security Management Act (FISMA) and Agency Privacy Management," dated April 21, 2010.

As of June 30, 2011, the Department reported a total of 162 systems in its inventory. The inventory consisted of 100 Department systems (the systems used by offices other than FSA) and 62 FSA systems. For these 162 systems, we identified that:

- 19 of 62 FSA systems were operating on interim ATOs.
- 28 of 100 Department systems were operating on expired ATOs.

OMB Memorandum M-10-15, FY 2010 Reporting Instructions for FISMA and Agency Privacy Management, dated April 21, 2010, states that OMB does not recognize interim authority to operate for security authorizations. NIST SP 800-37 guidance published in May 2004 included the use of interim ATOs on a more routine basis but the development of the guidance, as discussed in Issue 1a, de-emphasized the use of interim ATOs. NIST SP 800-37, Revision 1 does not discuss interim ATOs in the body of the guidance. However, footnote 68 states that some organizations may choose to use the term "interim ATO" to focus attention on the increased risk being accepted by the authorizing official in situations where there are significant weaknesses or deficiencies in the information system, but an overarching mission necessity requires placing the system into operation or continuing its operation. OCIO-05, "Handbook for Information Technology Security Certification and Accreditation Procedures," dated March 31, 2006, states that for accreditation decisions, if the Designated Approving Authority (DAA) deems that the risk is unacceptable but the operation of the system is essential to fulfill the mission of the Department, an interim ATO may be granted and should last no longer than 6 months. Further, OCIO-01, "Handbook for Information Assurance Security Policy," also dated March 31, 2006, provides that the DAA is responsible for ensuring that an interim ATO is granted only if the necessary security enhancements bring the system up to the acceptable level of risk. Although OCIO-05 and OCIO-01 speak to the DAA responsibilities regarding interim ATOs, the Department guidance has not been updated in accordance with NIST SP 800-37, Revision 1, to de-emphasize the use of interim ATOs and is not consistent with the intent of OMB. As a result, Department operations and assets can be exposed to significant security risks until significant security weaknesses are corrected or mitigated.

We identified the same issue in two previous audit reports. In a September 2008 report, the OIG found that FSA did not have controls in place to continuously monitor the Debt Management and Collection System (DMCS) between certification and accreditations (system authorizations) (Finding No. 1, Issue 1a).[6] In addition, FSA did not effectively manage the DMCS certification and accreditation program by monitoring and documenting the development, management, operation, and security of connections between DMCS and interfacing systems. Similar conditions exist in Issue 1b above. In an October 2009 report, the OIG found that FSA did not have controls in place to adequately manage authorization to operate because it had not updated the most recent system ATOs with the latest information from the accreditation decision (Finding No. 5).[7] Also, we found that FSA did not update changes to the SSP and other system documentation for the Postsecondary ED Participants System, Central Processing System (CPS), and National Student Loan Data System (NSLDS) (3 of 5 systems reviewed) (Finding No. 6). Similar conditions exist in Issue 1b above. Therefore, this is a Modified Repeat Condition.

[6] "IT Security Controls over the Debt Management Collection Process, Phase II, Fiscal Year 2008" (A11I0003), dated September 30, 2008.

[7] "Security over Certification and Accreditation for Information Systems" (A11J0001), dated October 13, 2009.

Consistent with our FISMA fieldwork, the EDUCATE audit team found that the Department did not establish an organization-wide risk management strategy. Although the OCIO and the system owners had performed application security risk assessments as part of the SSPs, the OCIO did not have an organization-wide risk management strategy as required by the OMB A-130 Appendices III and IV, and as clarified by NIST SP 800-39, "Managing Information Security Risk," dated March 2011. In addition, the EDUCATE audit team found that the system owners for CAMS, EDNIS, EDCAPS**,** and EDMASS needed to update security assessment and authorization documents.

Additionally, the OCIO did not ensure that the EDNIS security plan and update procedures needed to be revised to ensure full accountability of internal and external connections and to ensure all connecting systems were compliant with Federal information security requirements. The EDNIS SSP showed a list of 138 internal connections and 4 external connections. The SSP states that 109 of the 138 internal connections have been validated and 29 of the 138 internal connections have not been validated. Further, the EDNIS SSP disclosed that the 29 systems had the following deficiencies:

- 13 systems did not have an ISA or an MOU,
- 16 systems had not been reviewed within the past year,
- 10 systems had not been certified and accredited,
- 19 systems had outdated certification and accreditation, and
- 2 systems owners were not known.

Furthermore, for the four external connections, neither the EINSTEIN nor the Managed Security Service Provider (MSSP) intrusion detection systems had an MOU.[8] Additionally, the Treasury Financial Management System (TFMS) and the Department of Justice Cyber Security Assessment and Management (CSAM) MOU and ISA agreements had not been reviewed within the past 2 years. Further, the OCIO certification and accreditation documentation for EINSTEIN, MSSP, TFMS, and CSAM did not have a date to verify that the security authorizations were performed in the past 3 years.

In the EDUCATE report, we made 13 recommendations to the OCIO to address the risk management deficiencies cited above.

Recommendations

We recommend that the OCIO:

1.1 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.

[8] EINSTEIN is the US-CERT's automated process for collecting, correlating, analyzing, and sharing computer security information across the Federal government to improve our nation's situational awareness.

1.2 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).

1.3 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.

1.4 Develop controls to ensure timely re-authorizations for systems, avoiding gaps in ATO coverage.

1.5 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.

Management Response

The OCIO concurred with the finding and recommendations and made the following comments to specific statements in the Risk Management Finding.

Comment 1. Page 7 of the report inaccurately states that the FIPS 199 level in the Education's Security Tracking and Reporting System (EDSTAR) SSP did not match the FIPS 199 level in the FISMA FY 2011 Inventory (as of June 30, 2011). The Operational Vulnerability Management Solution (OVMS) categorizes EDSTAR as having a FIPS risk impact of "High." Additionally, the EDSTAR SSP (uploaded to OVMS on October 8, 2010) identifies this system as high.

Comment 2. Page 8 references previous audits "IT Security Controls over the Debt Management Collection Process, Phase II, Fiscal Year 2008" and "Security over Certification and Accreditation for Information Systems" in which similar security authorization issues were identified by the OIG. However, the report fails to include the corrective action taken by FSA to remediate the issues noted in these prior reports. FSA implemented continuous security authorization (CSA) to address the deficiencies noted in these audit reports and to improve their certification and accreditation program. FSA has enrolled 13 of its systems into the process; enrollment into CSA occurs only after a system completes a current Security Authorization that has baselined its controls for continued scheduled testing and monitoring in accordance with NIST requirements. The CSA process has been reviewed to the Department's CISO and is in the final stages of being formalized by FSA support contractors.

Comment 3. Page 9 of the report inaccurately states, "Neither the EINSTEIN nor the MSSP intrusion detection systems had an MOU." Attachment A (of Enclosure 3) provides a copy of the service level agreement that was entered into by DHS on June 9, 2011. Attachment B provides a copy of the MOU that was entered into by the Department's MSSP, Federal Aviation Administration and the Department on August 9, 2010. Also the Department of Justice Cyber Security Assessment and Management, noted by the OIG as not having an up-to-date MOU, was decommissioned in April 2010.

OIG Response

OCIO Comment 1 referred to the first bullet in Issue 1b. The OIG reviewed the most recent EDSTAR SSP posted in OVMS, which was dated March 2010. The SSP stated in section "2.2, FIPS 199 Security Categorization," that based on the severity of impact values identified for the Confidentiality, Integrity, and Availability, the overall security categorization (severity of impact) for this system is Moderate. The OIG verified that the most recent EDSTAR SSP posted in OVMS, as of October 13, 2011, is the March 2010 document reviewed as part of this report which categorizes the system as Moderate.

OCIO Comment 2 referred to our statements of prior OIG audit reports that contained findings with the same or similar conditions. Our purpose was to identify the prior audit findings as evidence that the repeat condition in this report had not been addressed enterprise-wide or organization-wide. See also the OIG Response in the Audit Results section above.

OCIO Comment 3 referred to findings restated from the EDUCATE audit report. We restated the EDUCATE findings in applicable controls areas because the findings from all reports issued by the OIG or GAO will be incorporated to answer the OMB CyberScope FISMA Report (Enclosure 1). The OCIO was given the opportunity to provide comments and additional evidence of compliance when the EDUCATE draft report was issued for management comments in August 2011. The OCIO did not provide the information cited in OCIO Comment 3 in management comments to the EDUCATE report. Because OCIO provided the document for the first time in response to this report, we have not had the opportunity to review and validate the information as it relates to the EDUCATE report finding.

FINDING NO. 2 – Configuration Management

Issue 2a - Patch Management Program Needs Improvement

Although the OIG issued reports that contained findings citing patch management deficiencies in each of the most recent 3 years, our current review found the OCIO still has not established and implemented formal, enterprise-wide patch management policy and procedures consistent with NIST requirements. NIST SP 800-53, Revision 3, Configuration Management (CM)-3 Configuration Change Control and System and Information Integrity (SI)-2 Flaw Remediation, require agencies to timely implement configuration control changes, such as the remediation of flaws, and to promptly install security-relevant software updates. Although the OCIO initiated development of the Vulnerability and Patch Management Policy, this policy was still in draft form as of June 2011. Without effective patch management procedures and processes 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.

The OIG identified this condition regarding the Department's patch management program in three previous audit reports. In a September 2008 report, the OIG reported that FSA needed to improve controls over risk assessment for DMCS and use scanning tools and techniques to identify and correct vulnerabilities, including needed patches (Finding No. 2).[9] In a June 2009 report, the OIG reported that the OCIO and the contractor did not protect all web sites by timely implementing updates and system patches (Finding No. 3).[10] In a September 2010 report, the OIG found that FSA did not ensure that the contractor performed patch management adequately and timely.[11] The conditions found in all three of these reports existed at EDUCATE and the OCIO program level. Therefore, this is a Modified Repeat Condition.

Issue 2b – Access Switch Port Security Needs Improvement

The contractor did not establish access switch port security for the switches within the enterprise network infrastructure, nor did it disable unused switch port connections.[12] As part of our audit fieldwork, we tested switch port security by successfully connecting a rogue computer asset to six Departmental local-area network (LAN) connections throughout a Department regional office. We conducted the test on August 10 and 11, 2011. During the test, OIG auditors installed a five-port CISCO switch on a LAN that was not detected or shutdown. Using the connections on the five-port CISCO switch, we were able to access web sites through the internet and remain undetected for more than 24 hours. Therefore, an unauthorized user could gain internal access to the Department's network by simply connecting a workstation or laptop to a wall plate or access point located in the work area. NIST and the Defense Information Systems Agency (DISA) Network Security Checklist (CISCO Layer 2 Switch) require that the information systems have all access switch ports secured.[13] The port security conditions occurred because the OCIO did not require the contractor to establish port security on access switch ports within the enterprise. As such, the OCIO's current security process is not consistent with NIST or DISA guidance. As a result, the OCIO and the contractor cannot prevent or detect rogue devices from being connected to the enterprise. Eliminating unauthorized access to the network from inside the enterprise is vital to keeping a network secure from introducing a virus, spyware, and malware.

The EDUCATE report also contained findings on configuration management. The EDUCATE audit team found that the Department's configuration management program needed improvement. Although Perot Systems performed monthly scans of the network, vulnerabilities in the security configuration continued to exist. For the 25 EDUCATE servers, switches, routers, and database configurations reviewed, the team identified the following significant high-risk configuration vulnerabilities:

- Four firewall systems had only one logon account each instead of unique user accounts for each individual accessing the systems to establish accountability and an audit trail.

[9] "IT Security Controls over the Debt Management Collection Process, Phase II, Fiscal Year 2008" (A11I0003), dated September 30, 2008.

[10] "Incident Handling and Privacy Act Controls over External Web Sites" (A11I0006), dated June 10, 2009.

[11] "Security Controls for Data Protection over the Virtual Data Center" (A11J0006), dated September 29, 2010.

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

[13] 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.

- Four Windows servers had anonymous shares that were not restricted, which allowed unauthorized network connections to the servers and enabled unauthorized systems to access shared information.
- One Windows server had unauthorized users with excessive operating system privileges that allowed them to execute operating system commands and bypass system's access controls.

Also, EDUCATE's hardware and software accountability security controls had the following deficiencies:

- Perot Systems reported 1,675 workstations with an undetermined operating system in the Perot Internet Protocol (IP) Scan, dated December 2010.
- Perot Systems could not identify the location of 2 of 10 UNIX servers sampled from a population of 363 servers. [14]
- In their monthly scan reporting process, neither the OCIO nor Perot Systems officials could explain why the December 2010 IP Scan report contained a tab titled "Servers" that listed 12 IP addresses as servers with unknown operating systems and unknown "Host name." Ten of the 12 IP addresses were also present on the IP Scan report for November of 2010.

In addition, the OCIO had not defined timeframes for installing security patches on network devices in the SLA with Perot Systems. The Perot Systems' patch management processes did not initially install critical security patches on network devices within the 3-day time period as required by the Dell End User Computing Workstation Patch and Configuration Management Process. In a sample of 25 devices consisting of 19 servers and 6 switches, Perot Systems had not installed critical security patches for 16 servers; however, Perot Systems had installed required security patches for the 6 switches. For two of the servers, the patches were not installed until 40 days after the release date. The OCIO was not aware that Perot Systems had not installed security patches on all network devices within the timeframe required by Dell's process (30 days).

Furthermore, Perot Systems network operating system controls for identifying and resolving vulnerabilities needed improvement. The team performed internal network vulnerability scans and identified the following high-risk vulnerabilities:

- Five Terminal Access Controller Access Control System Plus devices send authentication information in clear-text, which can be captured and used to logon to network devices.
- Nine network devices allow console connections without timeout settings. An attacker with physical access can connect to the console port using a non-terminated connection.
- One network device uses an unsecured service, remote login, which allows network administrators to login and send their credentials in clear-text, making them susceptible to packet analysis.

[14] Uniplexed Information and Computing System

- Nine network devices use Secure Shell Version 1 (SSH-1), which allows data to be exchanged using a secure channel. However, multiple vulnerabilities that exist make SSH-1 susceptible to man-in-the-middle attacks whereby an individual can capture data without detection.
- Four network devices use an unsecured service, Telnet, which allows network administrators to login and send their credentials in clear-text.
- Insecure library loading could allow remote code execution.
- Vulnerabilities in Server Message Block (SMB) server. For example, a specially crafted SMB packet sent to the affected system could allow remote code execution.

Additionally, the EDUCATE audit team identified that in 2010, the OCIO reported 15 Federal Desktop Core Configuration (FDCC) deviations in the OCIO Annual FISMA Report to OMB. Of the two deviations examined, the OCIO was not able to locate the authorization documentation related to either deviation.

In the EDUCATE report, we made 13 recommendations to the OCIO to address the configuration management deficiencies cited above.

Recommendations

We recommend the OCIO:

2.1 Develop, approve, and implement an enterprise-wide patch management policy that complies with OMB, NIST, and other applicable Federal guidelines.

2.2 Circulate and distribute the final approved patch management policy to all principal offices and contractors for consistent implementation.

2.3 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.[15]

2.4 Require the contractor to shutdown or disable unassigned/unused switch port connections throughout the enterprise.

Management Response

The OCIO concurred with Recommendations 2.1, 2.2, and 2.3. Management partially concurred with Recommendation 2.4 and stated:

The OCIO partially concurs with this recommendation. The Department CISO will issue a memorandum directing Dell to submit Risk Acceptance Forms (RAF) for unassigned/unused switch port connections on the Department’s network by October 21, 2011. These RAFs will be submitted to the CISO for approval.

[15] A network uplink is a path through the enterprise to the Internet.

Management also stated:

Page 12 inaccurately states, "The OCIO was not aware that Perot Systems had not installed security patches on all network devices within the timeframe required by Dell's process (30 days)." The Department receives a monthly report of non-installed patches from Dell.

OIG Response

The OCIO did not state with which part of Recommendation 2.4 it concurred and with which part it did not concur. It is unclear how the stated alternate activity will accomplish the intent of the recommendation since directing Dell to submit Risk Acceptance Forms to the CISO for approval does not constitute the act of disabling connections. The OCIO should implement the recommendation as stated.

With respect to OCIO's comment about an inaccurate statement on page 12, the OCIO was previously given the opportunity to provide comments and additional evidence of compliance when the EDUCATE draft report was issued for management comments in August 2011. The OCIO did not provide the information cited in management comments to the EDUCATE report. See Finding No. 1, Risk Management, OIG Response for OCIO Comment 3. We have not reviewed or validated additional information provided in response to this report.

FINDING NO. 3 – Incident Response and Reporting

In June 2011, the OIG's Technology Crimes Division issued an IPAR regarding the Department's incident response and reporting procedures. The OIG reported that investigations of potential computer crimes over the past 2 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," dated June 26, 2007, which is based on Federal guidelines and industry best practices.[16] The OIG reported these issues to the Department starting in March 2009. These failures prevented the collection of information that could aid the Department in identifying all compromised computers, the actions or vulnerability that enabled the incident, the objective of the incident, and the source. Additionally, the deficiencies left the Department's systems and data vulnerable. The OIG recommended the CIO enforce the contract's requirement for Perot Systems to comply with OCIO-14 when performing incident response or develop a separate capability to perform incident response in accordance with OCIO-14. The incident response capability, whether or not maintained by Perot Systems, should include:

- Providing incident response personnel with the appropriate training and tools to collect and preserve evidence in a quick and forensically sound manner (in person or remotely).
- Analyzing information to determine the root cause of an incident and to determine the extent of damage.

[16] OCIO-14, "Handbook for Information Security Incident Response and Reporting Procedures," was updated in March 2011.

- Implementing appropriate hardware, software, and procedures to activate full content network monitoring in a timely manner to support the incident response process and to assist in discovery of the incident's root cause.

Consistent with our previous OIG reporting, the EDUCATE audit team found that the Department's incident response program needed improvement to ensure timely and appropriate detection, reporting, and resolution of computer security incidents to external parties. Of the 15 incident tickets reviewed:

- Two of 15 security incidents pulled from OVMS were not reported to the US-CERT within a day of the occurrence. Specifically, one incident was not reported until 28 days after the incident, and another incident was reported 16 days after the incident. Both incidents were malicious code incidents.

- Four of 15 security incidents pulled from OVMS were not resolved in a timely manner to prevent further damage. Specifically, three of four security incidents, which were malicious code EINSTEIN alerts identified by US-CERT, were reported 14, 16, and 27 days after the incident; and one unauthorized access incident was reported 14 days late.

In the EDUCATE report, we recommended the OCIO require Perot Systems to comply with the EDUCATE SLA for resolving incidents within the SLA specified timeframe and continue its efforts to work with Perot Systems to address the issues cited in the IPAR, "Incident Response and Reporting Procedures," Control Number L21L0001.

Recommendation

We made no recommendations in addition to those contained in the IPAR and EDUCATE report cited above.

Management did not provide any comments for this finding.

FINDING NO. 4 – Security Training

Issue 4 - The OCIO Needs to Improve New User Security Training

The OCIO allowed new users access to the Department's network before they received IT security awareness and training. Pertinent guidance requires that new users receive IT security awareness and training before allowing them access to the systems.[17] The OCIO IT security awareness and training program policies were not updated to meet current FISMA guidance from OMB, the Office of Personnel Management (OPM), and NIST regarding new users. The outdated policies allowed new users to have network access and then to take the training within 10 working days of employment or, for contractor employees, within 10 working days of initiation of the applicable contract.

[17] OMB Circular A-130, Appendix III, November 28, 2000, as clarified by 5 C.F.R. §930.301 and NIST SP 800-53, Revision 3, dated August 2009.

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 policy, recognize IT security situations, and take appropriate steps to avert them. For the Department's programs to achieve their objectives, each individual who uses the Department's IT resources needs to assume responsibility for IT security.

Consistent with our FISMA fieldwork, the EDUCATE audit team found that the Department's security training program needed improvement. Specifically, the OCIO needed to improve documentation of security and awareness training. For instance, the OCIO could not provide supporting evidence for:

- Initial security and awareness training for 22 of 25 newly hired personnel. Additionally, documentation for 3 personnel of the 25 showed that the employees did not attend training within the 10-day period.
- Training records for all 25 employees selected who had significant information security responsibilities.

In the EDUCATE report, we made two recommendations to the OCIO to improve training documentation practices.

Recommendations

We recommend the OCIO:

4.1 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.

4.2 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.

Management Response

Management concurred with Recommendations 4.1 and 4.2.

FINDING NO. 5 – Plan of Action and Milestones

During the EDUCATE audit, the audit team found that the OCIO did not adequately manage the POA&M process and identified the following issues:

- The OCIO did not maintain an accurate inventory of the number of security control weaknesses identified from the monthly vulnerability scans, the number of previously reported security control weaknesses resolved in the period, and the number of actual or proposed remedial actions that management is currently working to resolve.

- Although the OCIO provides reports to Department management on the POA&M status of weaknesses identified during audits and reviews of A-123, Chief Financial Officer Financial Statement Audits, the OCIO did not provide management with all security weaknesses from its dashboard, specifically, contingency planning, annual assessment, certification and accreditation, and vulnerability scan findings.
- The OCIO did not monitor all security weaknesses in the POA&M reports and audit dashboard. Currently, the OCIO only records and monitors security control risks identified by the OIG.
- Security weaknesses identified during monthly network vulnerability scans were not reported in the POA&M OVMS database. The OCIO IA team receives these monthly vulnerability scans from Perot Systems and then analyzes them before inputting the weaknesses into the POA&M OVMS database.

In the EDUCATE report, we recommended the OCIO develop:

- Procedures to ensure that the POA&M program is maintained so that it always reflects the current status of open and closed POA&Ms.
- Procedures to monitor the remediation of all actions within the POA&M population.
- Procedures to estimate and record the resource requirements for implementing proposed corrective action in accordance with OMB Exhibits 53 and 300.
- An automated process to identify, track, maintain, and report security weaknesses resulting from the monthly vulnerability scans.

Recommendation

We made no recommendations in addition to those contained in the EDUCATE report cited above.

Management did not provide any comments for this finding.

FINDING NO. 6 – Remote Access Management

Issue 6a – Remote Access Policy Needs Improvement

The OCIO does not have comprehensive or complete remote access and telework security policies and procedures. Although there are a number of telework policy documents that address some NIST guidance, collectively the policies did not meet all the telework and remote access requirements. Specifically, the telework policy and procedures did not address how the organization's remote access servers are administered and how the policies in those servers are updated. NIST SP 800-53, Revision 3 and NIST SP 800-46, Revision 1, “Guide to Enterprise Telework and Remote Access Security,” issued June 2009, recommend that telework and remote access policy and procedures 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. Also, the organization should periodically perform assessments to confirm that the organization's remote access policies, processes, and procedures are being followed. The OCIO did not update the telework security and remote access policies and procedures to meet the standards outlined in the NIST guidance. As a result, remote access users do not have clear guidance to follow and may inadvertently increase the risk of unauthorized access to Department systems.

Issue 6b – Remote Access Controls, Settings, and Automated Restrictions Need Improvement

The OCIO did not have remote access management procedures and controls in place to address the following issues:

- Although users are not allowed to save to external devices, such as flash drives or compact discs (CDs), without using Department approved encryption, there was no technical or automated solution to enforce this restriction.
- Access through Citrix and FirePass did not time-out after 30 minutes of inactivity.
- New Citrix 2008 servers, brought on-line in February 2011, were not enabled to log connectivity activity and no logs were generated to be reviewed for indications of attacks or anomalies.
- Users are permitted to use non-government furnished equipment (GFE) devices to remotely connect to the EDUCATE network through FirePass, and can use a Citrix session to share the local computer drives (including any externally attached drive[s]). The ability to map to a non-GFE devices exposes the following three concerns: (a) users can copy files to the server and from the server; (b) the files downloaded from the server to the local device will be unencrypted if the user's non-GFE device is not encrypted; and (c) there is no control/restriction of the files being transferred over the connection.

OMB and NIST provide guidance for the remote access controls and management.

- NIST SP 800-53, Revision 3, provides standards to establish usage restrictions and implementation guidance, monitor for unauthorized remote access to the information system, authorize remote/wireless/mobile device access to the information system prior to connection, and enforce requirements for connections to the information system.[18]
- OMB recommends that agencies encrypt, using only NIST certified cryptographic modules, all data on mobile computers/devices carrying agency data unless the data are determined to be not sensitive, and use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes of inactivity.[19]
- NIST states that logging is a cornerstone of a sound security posture. Capturing the correct data in the logs and then monitoring those logs closely is vital. However, log files are often the only record of suspicious behavior. Enabling the mechanisms to log information allows the logs to be used to detect failed and successful intrusion attempts and to initiate alert mechanisms when further investigation is needed. Procedures and

[18] NIST SP 800-53, Revision 3, Access Control (AC)-17 Remote Access, AC-18 Wireless Access, and AC-19 Access Control for Mobile Devices.
[19] OMB M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," Attachment 1.C., Security Requirements, issued May 22, 2007.

tools need to be in place to process and analyze the log files and to review alert notifications. Also, server logs should be reviewed for indications of attacks.[20]

- NIST SP 800-46, Revision 1, states that an organization may choose to have tiered levels of remote access, such as allowing organization-owned computers to access many resources and teleworker-owned computer equipment allowed to access a limited set of resources. Additionally, an organization should have a policy of encrypting all sensitive data when it is at rest on the device and on removable media used by the device.

The Department's remote access control deficiencies occurred because the telework and remote access policies and procedures currently in place did not collectively provide all the necessary guidance to meet NIST standards. In addition, the Department did not develop and implement procedures and configuration settings in accordance with NIST guidance. Without adequate remote access controls, Department systems and data may be left unsecured and subject to attacks. These deficiencies could lead to data leakage or the introduction of malware into the network, which may compromise the user and the network, and allow attacks and other pertinent information to go unlogged and undetected.

Issue 6c – Two-Factor Authentication Not Fully Implemented

Although the OIG issued reports containing findings regarding the use of two-factor authentication for Federal employees and contractors in each of the most recent 3 years (FY 2008, FY 2009, and FY 2010), the OCIO still has not fully implemented and enforced the use of two-factor authentication when accessing the Department's systems.[21] Homeland Security Presidential Directive (HSPD)-12, dated August 27, 2004, required Federal agencies to use multi-factor authentication for access to information systems by October 27, 2005. OMB provided additional guidance for two-factor authentication for remote access. [22] The Department is currently in the process of implementing and enforcing the use of two-factor authentication for all Federal employees, contractors, and other authorized users. However, to date, this policy has not been fully implemented. According to FSA, the Department began issuing two-factor authentication protocol to all authorized users, including non-Federal users accessing FSA systems, during 2011 and plans to complete implementation by December 31, 2012. As a result of not fully implementing two-factor authentication, the Department cannot effectively account for and authenticate all users who access the network, which increases the risk of unauthorized access to privileged Department information. Also, because the Department uses single-factor authentication, malicious attackers could easily obtain and misuse the information from the Department's web sites or systems where large volumes of PII could be exfiltrated and Department data could be altered.

Consistent with our FISMA fieldwork, the EDUCATE audit team found that the OCIO did not ensure that the EDUCATE network software that controls remote access settings was compliant with OMB and NIST standards. The following deficiencies were identified:

[20] NIST SP 800-123, "Guide to General Server Security," dated July 2008.

[21] "IT Security Controls over the Debt Management Collection Process, Phase II, Fiscal Year 2008" (A11I0003), dated September 30, 2008; "Incident Handling and Privacy Act Controls over External Web Sites" (A11I0006), dated June 10, 2009; and IPAR – "Weaknesses in the Process for Handling Compromised Privileged Accounts" (L21K0002), dated September 16, 2010.

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

- The encryption algorithm for Department web sites does not comply with NIST SP 800-57, "Recommendation for Key Management Part 3: Application Specific Key Management Guidance," dated December 2009.
- The EDUCATE network does not require multifactor authentication to gain remote access as required by OMB Memorandums 06-16 "Protection of Sensitive Agency Information" dated, June 23, 2006, and 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," dated May 22, 2007. OMB requires agencies to allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.

In the EDUCATE report, we recommended that the OCIO require Perot Systems to change the digital certificate and bit encryption for remote servers to the recommended settings that are specified in NIST SP 800-57, Part 3 and expedite its efforts to work with Perot Systems to address the issues cited in the IPAR, "Weaknesses in the Process for Handling Compromised Privileged Accounts."

Recommendations

We recommend that the OCIO:

6.1 Develop policy and procedures that clearly define telework security and remote access requirements; types of remote access the organization permits; which types of devices are permitted to use each form of remote access; the type of access each type of teleworker is granted; how the remote access servers are to be administered; and how (automated) policies in those servers are to be updated.

6.2 Implement an automated enforcement or Endpoint/Media encryption solution that will automatically encrypt all information saved to external devices. [23]

6.3 Configure all remote sessions to time-out after 30 minutes of inactivity as mandated by OMB.

6.4 Configure the new Citrix 2008 servers to log connectivity activity and review these logs for indications of attacks or anomalies.

6.5 Configure EDUCATE Citrix to allow mapping only to GFE devices.

Management Response

The Department does not agree with the OIG's statement that Two-Factor Authentication (TFA) has not been implemented (Issue 6c). On August 31, 2011, the Department completed a project that required employees and contractors to use Personal Identity Verification cards to obtain

[23] Endpoint/Media encryption provides centrally enforceable encryption of removable storage media such as flash drives, backup hard drives, and CDs for maximum data protection. Port control enables management of all endpoint ports, plus centralized logging of port activity for auditing and compliance.

access to the Department's network. On September 19, 2011, the Department went into a disaster recovery mode that temporarily allowed the use of username and password.

The Department currently requires TFA for FSA users and has current plans to require TFA for all employees and contractors. On May 17, 2011, FSA made TFA mandatory for employees accessing the FSA version of Citrix remotely. On October 25, 2011, the rest of the Department will be required to use TFA when remotely connecting to the ED.gov version of Citrix.

FSA has initiated a pilot with seven foreign schools and is in the process of implementing TFA at certain pre-identified continental United States schools. FSA anticipates full implementation of TFA for all external partners by September 30, 2012.

The OCIO concurred with Recommendations 6.1, 6.2, 6.3, and 6.4. The OCIO did not concur with Recommendation 6.5 and stated:

Configuring CITRIX to map only to GFE without additional architectural changes will impede mission critical functions and the ability to implement telework in accordance with OMB guidance. The OCIO has implemented TFA for the EDUCATE CITRIX capability and is working on additional architectural changes to enhance the security capability and policy for remote access.

OIG Response

The OCIO stated that it does not agree that two-factor authentication has not been implemented and states actions taken and planned toward implementation. However, in Issue 6c, we stated that full implementation has not occurred and according to the OCIO's statements, full implementation including system access by external partners is not scheduled until September 2012. The OCIO has not implemented two-factor authentication for all personnel that require it, and for those parts recently implemented, it did not have controls in place for a length of time so that implementation can be verified as consistently applied. See also the OIG Response in the Audit Results section above.

Regarding Recommendation 6.5, the OCIO did not provide any details about how implementing NIST guidance will impede mission critical functions and the ability to implement telework in accordance with OMB guidance. The OCIO's reference to implementation of TFA is a separate issue and does not provide the protection that properly configuring Citrix according to Recommendation 6.5 can provide. We made no changes to Recommendation 6.5 based on management's comments.

FINDING NO. 7 – Identity and Access Management

Issue 7 - The Identity and Access Management Program Needs Improvement

The OCIO did not have fully developed processes for identity and access management. Specifically, we found that the OCIO did not have processes 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 the information system uniquely identifies and authenticates users and specific devices before establishing a connection. The OCIO did not establish and implement policies and procedures to be consistent with NIST requirements for establishing and maintaining effective identity and access management. Without the ability to account for and authenticate all devices connected to the network, the Department cannot effectively monitor, track, and authenticate all devices and users of the devices. Also, without proper logical access control in place, the Department cannot ensure that the identification and authentication controls are operating as intended and preventing unauthorized transactions or functions. Consequently, the Department's information is vulnerable to local attacks that could lead to a loss of confidentiality caused by unauthorized access to data and to a possible loss of integrity through data modification or limited availability from unauthorized access and excessive use of system resources.

The Department is planning, engineering, and budgeting for an enterprise-wide identity management capability that will provide more granular and centrally managed identity and access management controls for EDUCATE, VDC, and major system applications. Planning is currently underway and implementation is funded in the FY 2013 budget.

Consistent with our FISMA fieldwork, the EDUCATE audit team found that the Department's identity and access management process needed significant improvement. Based on tests of 6,997 active accounts in the Active Directory user account management functions, the following deficiencies were identified:

- 71 of 170 accounts established for training purposes had not been used since January 2010.
- 1,000 accounts had never been logged on to the network. According to EDNIS and the EDCIS SSPs, accounts that have not logged on to the EDCIS and EDNIS for more than 90 days should have been deactivated.
- 221 user accounts had their password settings checked as "Do Not Expire" in the Active Directory. Of the 221 accounts, 53 were Service Accounts.[24] The EDCIS SSP states that password expiration should be enabled for all users.
- 80 active accounts had not changed their password since January 1, 2010. According to EDCIS SSP, all users are required to periodically change their password.

In addition, from a population of 37 voluntarily separated employees, management had not disabled the accounts of 9 of these employees within the 2-day requirement.

[24] Service Accounts are software utility accounts that permit the software to automatically communicate and authenticate with other software and computers on the domain in a secure mode. Service accounts are powerful and highly useful accounts that must be properly secured to prevent exploitation.

In the EDUCATE report, we recommended the OCIO ensure that the Active Directory is annually reviewed for access privileges of users, configure the Active Directory account management automated tools to flag accounts that have not been used, ensure that all accounts are configured with passwords that have an expiration date, and revise the SLA to include a performance incentive or penalty clause to enforce the OCIO account management policies.

The OIG identified this condition regarding the Department's identity and access management program in a previous audit report. In a September 2010 report, Issue 3b, the OIG found that FSA did not accurately manage inactive user accounts.[25] Specifically, inactive account settings did not follow FSA policy for disabling accounts after 90 days of inactivity or were set to never disable/deactivate. This is a Repeat Condition.

Recommendation

7.1 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.

Management Response

Management identified corrective actions taken in response to the EDUCATE report and concurred with Recommendation 7.1.

FINDING NO. 8 – Contingency Planning

Issue 8 – Contingency Planning Needs Improvement

The OCIO relied on contingency plans that were not complete or were missing required elements. Specifically, 9 of 16 systems reviewed did not include all the required contingency planning elements identified in NIST and Department guidance.[26] For example, 4 of the 16 systems' contingency plans were missing information regarding the use of an alternate telecommunications service that would be used if an event occurred that required relocation to the alternate site. This occurred because the OCIO did not include all the required elements in accordance with NIST requirements for developing effective contingency plans. 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 and effectively following a service disruption or disaster.

[25] "Security Controls for Data Protection over the Virtual Data Center" (A11J0006), dated September 29, 2010.

[26] NIST SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems," dated May 2010, and OCIO-10, "Handbook for Information Technology Security Contingency Planning Procedures," dated July 12, 2005.

We identified the same issue in two previous audit reports. In an October 2009 report, the OIG reported findings regarding the contingency planning process for CPS, NSLDS, and VDC. [27] In addition, in a September 2010 report, the OIG found that FSA did not adequately manage contingency planning for telecommunications services (Issue 7b). [28] Specifically, FSA did not request telecommunication service priority (TSP) for national security emergency preparedness and did not include TSP requirements in the VDC Telecommunications Plan. Therefore, this is a Repeat Condition.

Consistent with our FISMA fieldwork, the EDUCATE audit team found that the Department's contingency planning program needed improvement. Specifically, supporting documentation for SSPs, risk assessments, Business Impact Analysis (BIA), Disaster Recovery Plans (DRP), Continuity of Operation Plans (COOP), and Business Contingency Plans (BCP) contained the following deficiencies:

- The OCIO had not documented an entity-wide BIA to support the EDUCATE contingency plans to ensure coordination of the recovery of critical mission/business processes and services in the event of a disruption.
- The OCIO in conjunction with Perot Systems had not developed contingency plans for EDNIS, EDMASS, CAMS, and EDSOC.
- The OCIO, and Perot Systems, had not conducted disaster recovery functional exercises such as table-top exercises within the past year as required by "OCIO-01 Handbook" and "OMB Circular A-130 Appendix III" as reflected in NIST SP 800-53, Revision 3 and 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems," dated May 2010 for EDNIS, EDMASS, EDSOC, and CAMS.
- The OCIO had not requested TSP codes for National Security Emergency Preparedness as required by the Department of Homeland Security. These codes are necessary to permit the resumption of information system operations for essential missions and business functions when the primary telecommunications capabilities are unavailable.

In the EDUCATE report, we made four recommendations to the OCIO to address the contingency planning deficiencies cited above.

Recommendation

8.1 We recommend that the OCIO review and update system contingency plans for the nine systems that have elements missing (list provided to the OCIO) to ensure that all the required contingency planning elements are included as required by NIST guidance.

Management Response

Management identified corrective actions taken in response to the prior audits cited in this finding and stated additional planned corrective actions. Management concurred with Recommendation 8.1.

[27] "Security over Certification and Accreditation for Information Systems" (A11J0001), dated October 13, 2009.
[28] "Security Controls for Data Protection over the Virtual Data Center" (A11J0006), dated September 29, 2010.

FINDING NO. 9 – Contractor Systems

Issue 9 – Contract Monitoring Controls Need Improvement

The OMB IG metrics for the Contractor Systems area asked that we assess whether the Department has established and maintains a program to oversee systems operated on its behalf by contractors or other entities that includes the following attributes:

- Documented policies and procedures for information security oversight of systems operated on the agency's behalf by contractors or other entities to include contract monitoring.
- The agency obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and agency guidelines.
- A complete inventory of systems operated on the agency's behalf by contractors or other entities.
- The inventory identifies interfaces between these systems and agency-operated systems.
- The agency requires appropriate agreements (e.g., MOUs, ISAs, contracts, etc.) for interfaces between these systems and those that it owns and operates.
- The inventory of contractor systems is updated at least annually.
- Systems that are owned or operated by contractors or entities are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.

The Department's system inventory, as of June 30, 2011, showed 162 total systems, consisting of 114 contractor-operated systems and 48 agency-operated systems. Whether contractor-operated or agency-operated, the Department requires IT systems to meet the security requirements set forth by FISMA, OMB, and NIST. We assessed the Department's oversight of IT systems as a whole by reviewing the attributes listed above and did not identify deficiencies that were specific to the systems being contractor-operated. However, all of the deficiencies identified in Finding Nos. 1 through 8 affect or apply to all Department systems, whether contractor-operated or agency-operated systems.

In a February 2011 report regarding the Department's need for improved oversight and controls to respond to its evolving priorities, GAO found that the Department developed overall guidance directed at maintaining financial accountability over two of its challenging resource management areas—contract monitoring and Pell Grants.[29] However, the Department had not yet developed and implemented detailed procedures for all control activities essential to ensuring that its contract monitoring policy directives are effectively carried out, including conducting supervisory reviews and documenting contract monitoring activity. Such deficiencies could impair the Department's ability to maintain effective financial accountability over its significant contract resource investment. GAO's review of internal controls over the Department's Pell Grants program did not identify any flaws in its overall design.

To help improve contract monitoring controls, GAO recommended that the Secretary of Education direct the Chief Operating Officer of FSA to take the following three actions:

[29] "Department of Education: Improved Oversight and Controls Could Help Education Better Respond to Evolving Priorities," dated February 2011 (GAO-11-194), Finding 3, Education Has Policies over Contract Monitoring and Pell Grants, but FSA's Contract Monitoring Procedures are Insufficient.

- Develop procedures that detail how to file and retain evidence demonstrating receipt and acceptance of contracted goods and services.
- Develop procedures that outline how contract monitoring activities and results should be documented, retained, and shared.
- Develop comprehensive quality control procedures that include guidance for review of contract files and contractor past performance reports to ensure that files are complete and contain documentation to evidence compliance with Department contracting policies, including contractor performance evaluations, contract monitoring plans, and contracting officers' representative appointment memoranda.

Recommendation

We made no recommendations in addition to those contained in the GAO report cited above or in Finding Nos. 1 through 8 of this report.

Management did not provide any comments for this finding.

FINDING NO. 10 – Security Capital Planning

Issue 10 – Security Capital Planning Needs Improvement

The OMB IG metrics for the Security Capital Planning area asked that we assess whether the Department has established and maintains a security capital planning and investment program for information security that includes 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.
- Discrete line items for information security in organizational programming and documentation.
- Employment of a business case to record the information security resources required.
- Availability of information security resources for expenditures as planned.

We assessed the Department's documented policies and procedures for the capital planning and investment control process. The process is governed by the E-Government Act, FISMA, Clinger-Cohen Act of 1996, and OMB Circulars, among other laws and regulations. The Department's guides and handbooks cite these applicable laws and follow the guidance and objectives provided. The Investment and Acquisition Management Team, of the Enterprise Architecture group meets to review all aspects of the capital planning and investment process, which includes going over the security requirements. The Planning and Investment Review Working Group (PIRWG) holds system owner presentation meetings that culminate in a deliberation session where the PIRWG decides on funding levels they recommend to the Investment Review Board for approval. Approved IT investment packages continue in the process to be funded. The process is designed to ensure investments in IT effectively support the mission of the Department in an orderly process. We did not identify any deficiencies in the documented policies and procedures and, due to time constraints, we did not evaluate the implementation or effectiveness of these documented controls. Additionally, we did not assess the Department's use of discrete line items, information security resources business cases, or how resource availability was enforced.

In the February 2011 report, GAO found that although the Department had developed key IT management controls, challenges still remained regarding planning and investment management.[30] More specifically, although the Department had developed an information resources management (IRM) strategic plan as required, it did so prior to the development of an updated Department strategic plan and without incorporating the IT goals from other key planning documents. In addition, the Department established controls to evaluate its IT investments, but it had not conducted postimplementation reviews as required. Unless the Department has an IRM strategic plan that is aligned with and informed by the current Department-wide strategic plan, the Department may not comprehensively and effectively support its mission. If the Department does not conduct postimplementation reviews for IT investments, it cannot effectively incorporate experiences and lessons learned from system development efforts that may improve the agency's overall IT investment management process.

GAO recommended that the Secretary of Education build on the Department's IT management efforts by directing the CIO to take the following three actions:

- Ensure that during the strategic planning process, the IRM strategic plan is aligned with and informed by the Department's strategic plan to eliminate any potential risk of major IT investments not supporting the Department's most current priorities.
- Update the IRM strategic plan to reflect goals from the Open Government, Strategic Sustainability Performance, and Data Center Consolidation plans.
- Finalize and approve Department guidance for implementing postimplementation reviews and conduct these reviews, where appropriate, to assess lessons learned and identify potential improvements to the IT management process.

Recommendation

We made no recommendations in addition to those contained in the GAO report cited above.

Management did not provide any comments for this finding.

[30] Finding 4, Education Has Established Important Information Technology Management Controls, but Planning and Investment Management Challenges Remain.

OTHER MATTERS

During port security tests, discussed in Finding No. 2, Issue 2b, we also identified two physical security deficiencies in a Department regional office. Specifically, on August 10 and 11, 2011, auditors found that the Department's VTC room was unsecured and unattended, and the communications room was easily accessed through a door with a partially disabled lock.

The OIG selected the office space for testing and evaluation because it is accessible by the general public. The floors have video cameras that the building's security contractor operates and maintains, and which generally are reviewed only after a known incident has occurred.

Physical Security Deficiency 1

The Department's VTC was left open and unattended while a video conference was being conducted. This condition could allow unauthorized persons access to sensitive information. During both days of our test, the auditors made several trips to the VTC facility and noted that the conditions in the room did not change and that the room was still unsecured. Toward the end of the business day on each test day, the auditors closed the door to the VTC room and ensured that it was secure.

Physical Security Deficiency 2

The Main Distribution Frame (MDF) room is situated in the middle of the building and has two doors, one on each end. The primary door (the one that has the room number labeling) is a reinforced door and did not exhibit any obvious deficiencies when checked. The secondary door exhibited an immediate and obvious problem when checked. The secondary door moved inward approximately ½ to ¾ of an inch exposing the locking mechanism arm. This clearly indicated that it could be manipulated in such a way that the door could be opened with little effort. The auditors were able to open the door within seconds. Once inside, auditors discovered the room housed the MDF, which supplies internet and telephone service throughout the Department's regional office. These conditions were unchanged as of August 31, 2011.

The OIG notified applicable Department officials, including those in the OCIO, of these conditions on September 6, 2011.

<u>Management Comment</u>

Management stated that corrective action was taken for Physical Security Deficiency 2 on October 7, 2011. The OIG verified that the MDF room door lock was in working order on October 12, 2011.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of our audit 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, "Federal Information Security Management Act," and 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.

For FY 2011 FISMA reporting, each IG is required to evaluate their respective agency, based on OMB guidance, on the following security areas:

- Risk Management
- Configuration Management
- Incident Response and Reporting
- Security Training
- POA&M
- Remote Access Management
- Identity and Access Management
- Continuous Monitoring Management
- Contingency Planning
- Contractor Systems
- Security Capital Planning

For FY 2011 FISMA reporting, we selected 16 systems for review. Of the 16 systems selected, we included 7 from the judgmental sample performed as part of our FY 2010 review. We selected these systems in order to measure progress from the prior fiscal year. The remaining 9 systems were judgmentally selected based on the system risk level of moderate or high from Department PO components that managed greater numbers of systems. The table below lists the systems selected, the system's PO, the FIPS 199 potential impact level (Level), and whether the system was selected as a repeat system from our FY 2010 review, or was a new selection as part of our FY 2011 review. We used this sample to evaluate the security areas of Risk Management, Configuration Management, Identity and Access Management, and Contingency Planning. While we reviewed whether specific security controls were implemented at 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	PO	Level	Initial FY Selection
1	Virtual Data Center	FSA	High	2011
2	National Student Loan Data System	FSA	Moderate	2011
3	Common Origination and Disbursement	FSA	Moderate	2011
4	Operational Vulnerability Management Solution	FSA	Moderate	2011
5	ED.gov	OCIO	Moderate	2011
6	Presidential Scholars Program Electronic Application	OCO	Moderate	2010
7	Case and Activity Management System	OCR	Moderate	2011
8	ED Investigative Tracking System	OIG	Moderate	2011
9	Management Information System	OIG	Moderate	2010
10	EDSTAR ID/Access System	OM	High	2010
11	Teacher Quality Enhancement Title II Scholarship and Administration Reporting System	OPE	Moderate	2010
12	Jacob K. Javits Fellows Database	OPE	Moderate	2011
13	EDFacts	OPEPD	Moderate	2010
14	Correspondence Control Manager Plus	OS	Moderate	2010
15	Case Services Reporting System	OSERS	Moderate	2011
16	National Center on Service Obligation Scholar Tracking System	OSERS	Moderate	2010

In addition to our FISMA fieldwork, we have incorporated the results of other OIG products into this year's FISMA review. These products include the EDUCATE information security audit and an Investigative Program Advisory Report.[31]

EDUCATE 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 the Department had developed and implemented adequate information systems security controls to properly safeguard EDUCATE and the Department's data in accordance with FISMA, OMB, and NIST regulations and standards. The audit team concluded that the Department's information systems security program controls over EDUCATE need improvement to address 14 operational, managerial, and technical security control risks identified during the audit.

Investigative Program Advisory Report

In June 2011, the OIG reported that investigations of potential computer crimes over the past 2 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 Department's OCIO-14, "Handbook for Information Security Incident Response and Reporting

[31] "Education Department Utility for Communications, Applications, and Technology Environment Information Security Audit," Control No. ED-OIG/A11L0001, dated September 30, 2011. "Incident Response and Reporting Procedures (10-110283)," Control No. L21L0001, dated June 14, 2011.

Procedures," which is based on Federal guidelines and industry best practices. The OIG reported these issues to the Department starting in March 2009. These failures prevented the collection of information that could aid the Department in identifying all compromised computers, the actions or vulnerability that enabled the incident, the objective of the incident, and the source. Additionally, they left the Department's systems and data vulnerable.

This audit covered the Department's management of IT security programs and systems for FY 2011. The audit included Department-wide and IT system audits completed and on-going during FY 2011. Fieldwork was conducted from February 2011 through August 2011, 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 2008 to the present. We will hold an exit conference with OCIO and FSA officials on October 6, 2011. We provided an official draft report on October 5, 2011.

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.
- Analyzed the security and awareness training (standard and specialized) courses and content. Reviewed and analyzed spreadsheets of Department and FSA standard and specialized security and awareness training for FY 2011.
- Reviewed Department and contractor systems' security plans, continuity of services plans, contingency plans, configuration management plans, and remote access and system user procedures.
- 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

2011

Annual FISMA Report

Department of Education

Section 1: Risk Management

1.b. **The Agency has established and is maintaining a risk management program. However, the Agency needs to make significant improvements as noted below.**

Comments: “The U.S. Department of Education’s Compliance with the Federal Information Security Management Act for Fiscal Year 2011,” Audit Control No. ED-OIG/A11L0003, hereafter referred to as FISMA Report.
“Education Department Utility for Communications, Applications, and Technology Environment Information Security Audit,” Audit Control No. ED-OIG/A11L0001, hereafter referred to as EDUCATE Report.
“Incident Response and Reporting Procedures (10-110283),” Control No. L21L0001, hereafter referred to as IPAR “Incident Response and Reporting Procedures.”

1.b(1). **Risk Management policy is not fully developed.**

Yes

Comments: FISMA Report: Finding No. 1, Risk Management, Issue 1a, OCIO Needs to Fully Implement the Risk Management Program.
EDUCATE Report: Finding No. 12, Department Needed to Establish an Organization-Wide Risk Management Strategy.

1.b(2). **Risk Management procedures are not fully developed, sufficiently detailed (SP 800-37, SP 800-39, SP 800-53).**

Yes

Comments: FISMA Report: Finding No. 1, Risk Management, Issue 1a, OCIO Needs to Fully Implement the Risk Management Program.
EDUCATE Report: Finding No. 12, Department Needed to Establish an Organization-Wide Risk Management Strategy.

1.b(3). **Risk Management procedures are not consistently implemented in accordance with government policies (SP 800-37, SP 800-39, SP 800-53).**

Yes

For Official Use Only

Comments: FISMA Report: Finding No. 1, Risk Management, Issue 1b - The OCIO Needs to Improve the System Authorization Process.
EDUCATE Report: Finding No. 8, EDNIS Security Plan and Update Procedures Needed to Be Revised to Ensure Full Accountability of Internal and External Connections and to Ensure All Connecting Systems Are Compliant with Federal Information Security Requirements.
EDUCATE Report: Finding No. 10, The Department Needed to Update the Security Assessment and Authorization Documents.

1.b(4). **A Comprehensive governance structure and Agency-wide risk management strategy has not been fully developed in accordance with government policies (SP 800-37, SP 800-39, SP 800-53).**

Yes

Comments: FISMA Report: Finding No. 1, Risk Management, Issue 1a, OCIO Needs to Fully Implement the Risk Management Program.
EDUCATE Report: Finding No. 12, Department Needed to Establish an Organization-Wide Risk Management Strategy.

1.b(5). **Risks from a mission and business process perspective are not addressed (SP 800-37, SP 800-39, SP 800-53).**

Yes

Comments: FISMA Report: Finding No. 1, Risk Management, Issue 1a, OCIO Needs to Fully Implement the Risk Management Program.
EDUCATE Report: Finding No. 12, Department Needed to Establish an Organization-Wide Risk Management Strategy.

1.b(6). **Information systems are not properly categorized (FIPS 199/SP 800-60).**

No

Comments: No exceptions noted.

1.b(7). **Appropriately tailored baseline security controls are not applied to information systems in accordance with government policies (FIPS 200/SP 800-53).**

No

Comments: No exceptions noted.

1.b(8). **Risk assessments are not conducted in accordance with government policies (SP 800-30).**

Yes

Comments: FISMA Report: Finding No. 1, Risk Management, Issue 1a, OCIO Needs to Fully Implement the Risk Management Program.
EDUCATE Report: Finding No. 12, Department Needed to Establish an Organization-Wide Risk Management Strategy.

1.b(9). **Security control baselines are not appropriately tailored to individual information systems in accordance with government policies (SP 800-53).**

No

Comments: No exceptions noted.

1.b(10). **The communication of information system specific risks, mission/business specific risks and organizational level (strategic) risks to appropriate levels of the organization is not in accordance with government policies.**

No

Comments: No exceptions noted.

1.b(11). **The process to assess security control effectiveness is not in accordance with government policies (SP800-53A).**

Yes

Comments: FISMA Report: Finding No. 1, Risk Management, Issue 1a, OCIO Needs to Fully Implement the Risk Management Program.
EDUCATE Report: Finding No. 12, Department Needed to Establish an Organization-Wide Risk Management Strategy.

1.b(12). **The process to determine risk to Agency operations, Agency assets, or individuals, or to authorize information systems to operate is not in accordance with government policies (SP 800-37).**

No

Comments: No exceptions noted.

1.b(13). **The process to continuously monitor changes to information systems that may necessitate reassessment of control effectiveness is not in accordance with government policies (SP 800-37).**

Yes

Section 1: Risk Management

Comments: FISMA Report: Finding No. 1, Risk Management, Issue 1a, OCIO Needs to Fully Implement the Risk Management Program.
EDUCATE Report: Finding No. 12, Department Needed to Establish an Organization-Wide Risk Management Strategy.

1.b(14). **Security plan is not in accordance with government policies (SP 800-18, SP 800-37).**

Yes

Comments: FISMA Report: Finding No. 1, Risk Management, Issue 1b - The OCIO Needs to Improve the System Authorization Process.
EDUCATE Report: Finding No. 12, Department Needed to Establish an Organization-Wide Risk Management Strategy.

1.b(15). **Security assessment report is not in accordance with government policies (SP 800-53A, SP 800-37).**

No

Comments: No exceptions noted.

1.b(16). **Accreditation boundaries for Agency information systems are not defined in accordance with government policies.**

No

Comments: No exceptions noted.

1.b(17). **Other**

No

Comments: No exceptions noted.

Section 2: Configuration Management

2.b. **The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make significant improvements as noted below.**

2.b(1). **Configuration management policy is not fully developed (NIST 800-53: CM-1)**

Yes

Section 2: Configuration Management

Comments: FISMA Report: Finding No. 2, Configuration Management, Issue 2a - Patch Management Program Needs Improvement.
EDUCATE Report: Finding No. 1, Security Configuration Management Process Needed Improvement.

2.b(2). Configuration management procedures are not fully developed (NIST 800-53: CM-1).

Yes

Comments: FISMA Report: Finding No. 2, Configuration Management, Issue 2a - Patch Management Program Needs Improvement.
EDUCATE Report: Finding No. 1, Security Configuration Management Process Needed Improvement.

2.b(3). Configuration management procedures are not consistently implemented (NIST 800-53: CM-1).

Yes

Comments: FISMA Report: Finding No. 2, Configuration Management, Issue 2a - Patch Management Program Needs Improvement.
FISMA Report: Finding No. 2, Issue 2b Access Switch Port Security Needs Improvement.
EDUCATE Report: Finding No. 1, Security Configuration Management Process Needed Improvement.
EDUCATE Report: Finding No. 2, Network Security Controls over Hardware Devices and Software Needed Improvement.
EDUCATE Report: Finding No. 3, Security Patch Management Process Needed Improvement.
EDUCATE Report: Finding No. 4, Remote Access Software Was Not Compliant with OMB and NIST Standards.
EDUCATE Report: Finding No. 5, Controls for Identifying and Resolving Vulnerabilities Needed Improvement.

2.b(4). Standard baseline configurations are not identified for software components (NIST 800-53: CM-2).

No

Comments: No exceptions noted.

2.b(5). Standard baseline configurations are not identified for all hardware components (NIST 800-53: CM-2).

No

Comments: No exceptions noted.

2.b(6). Standard baseline configurations are not fully implemented (NIST 800-53: CM-2).

No

Section 2: Configuration Management

Comments: No exceptions noted.

2.b(7). **FDCC/USGCB is not fully implemented (OMB) and/or all deviations are not fully documented (NIST 800-53: CM-6).**

Yes

Comments: EDUCATE Report: Finding No. 9, Federal Desktop Core Configuration Security Configuration Management Process Needed Improvement.

2.b(8). **Software assessing (scanning) capabilities are not fully implemented (NIST 800-53: RA-5, SI-2).**

No

Comments: No exceptions noted.

2.b(9). **Configuration-related vulnerabilities, including scan findings, have not been remediated in a timely manner, as specified in Agency policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2).**

Yes

Comments: EDUCATE Report: Finding No. 5, Controls for Identifying and Resolving Vulnerabilities Needed Improvement.

2.b(10). **Patch management process is not fully developed, as specified in Agency policy or standards. (NIST 800-53: CM-3, SI-2).**

Yes

Comments: FISMA Report: Finding No. 2, Configuration Management, Issue 2a - Patch Management Program Needs Improvement.
EDUCATE Report: Finding No. 3, Security Patch Management Process Needed Improvement.

2.b(11). **Other**

No

Comments: No exceptions noted.

Section 3: Incident Response and Reporting

3.b. **The Agency has established and is maintaining an incident response and reporting program. However, the Agency needs to make significant improvements as noted below.**

3.b(1). **Incident response and reporting policy is not fully developed (NIST 800-53: IR-1).**

No

Comments: No exceptions noted.

3.b(2). **Incident response and reporting procedures are not fully developed or sufficiently detailed (NIST 800-53: IR-1).**

No

Comments: No exceptions noted.

3.b(3). **Incident response and reporting procedures are not consistently implemented in accordance with government policies (NIST 800-61, Rev1).**

Yes

Comments: IPAR: “Incident Response and Reporting Procedures” Finding No. 1, The Department has not Detected, Reported, or Responded Appropriately to Security Incidents.
EDUCATE Report: Finding No. 6, Department’s Incident Response Program Needed Improvement.

3.b(4). **Incidents were not identified in a timely manner, as specified in Agency policy or standards (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).**

Yes

Comments: IPAR: “Incident Response and Reporting Procedures” Finding No. 1, The Department has not Detected, Reported, or Responded Appropriately to Security Incidents.
EDUCATE Report: Finding No. 6, Department’s Incident Response Program Needed Improvement.

3.b(5). **Incidents were not reported to US-CERT as required (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).**

Yes

Comments: IPAR: “Incident Response and Reporting Procedures” Finding No. 1, The Department has not Detected, Reported, or Responded Appropriately to Security Incidents.
EDUCATE Report: Finding No. 6, Department’s Incident Response Program Needed Improvement.

3.b(6). **Incidents were not reported to law enforcement as required (SP 800-86).**

No

Comments: No exceptions noted.

3.b(7). **Incidents were not resolved in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).**

Yes

Section 3: Incident Response and Reporting

Comments: IPAR: “Incident Response and Reporting Procedures” Finding No. 1, The Department has not Detected, Reported, or Responded Appropriately to Security Incidents.
EDUCATE Report: Finding No. 6, Department’s Incident Response Program Needed Improvement.

3.b(8). **Incidents were not resolved to minimize further damage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).**

Yes

Comments: IPAR: “Incident Response and Reporting Procedures” Finding No. 1, The Department has not Detected, Reported, or Responded Appropriately to Security Incidents.
EDUCATE Report: Finding No. 6, Department’s Incident Response Program Needed Improvement.

3.b(9). **There is insufficient incident monitoring and detection coverage in accordance with government policies (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).**

Yes

Comments: IPAR: “Incident Response and Reporting Procedures” Finding No. 1, The Department has not Detected, Reported, or Responded Appropriately to Security Incidents.
EDUCATE Report: Finding No. 6, Department’s Incident Response Program Needed Improvement.

3.b(10). **The Agency cannot or is not prepared to track and manage incidents in a virtual/cloud environment.**

No

Comments: No exceptions noted.

3.b(11). **The Agency does not have the technical capability to correlate incident events.**

No

Comments: No exceptions noted.

3.b(12). **Other**

No

Comments: No exceptions noted.

Section 4: Security Training

4.b. **The Agency has established and is maintaining a security training program. However, the Agency needs to make significant improvements as noted below.**

Section 4: Security Training

4.b(1). **Security awareness training policy is not fully developed (NIST 800-53: AT-1).**

No

Comments: No exceptions noted.

4.b(2). **Security awareness training procedures are not fully developed and sufficiently detailed (NIST 800-53: AT-1).**

Yes

Comments: FISMA Report: Finding No. 4, Issue 4 - The OCIO Needs to Improve New User Security Training.
EDUCATE Report: Finding No. 13, Documentation of Security Awareness Training Needed Improvement.

4.b(3). **Security awareness training procedures are not consistently implemented in accordance with government policies (NIST 800-53: AT-2).**

Yes

Comments: FISMA Report: Finding No. 4, Issue 4 - The OCIO Needs to Improve New User Security Training.
EDUCATE Report: Finding No. 13, Documentation of Security Awareness Training Needed Improvement.

4.b(4). **Specialized security training policy is not fully developed (NIST 800-53: AT-3).**

No

Comments: No exceptions noted.

4.b(5). **Specialized security training procedures are not fully developed or sufficiently detailed in accordance with government policies (SP 800-50, SP 800-53).**

No

Comments: No exceptions noted.

4.b(6). **Training material for security awareness training does not contain appropriate content for the Agency (SP 800-50, SP 800-53).**

No

Comments: No exceptions noted.

4.b(7). **Identification and tracking of the status of security awareness training for personnel (including employees, contractors, and other Agency users) with access privileges that require security awareness training is not adequate in accordance with government policies (SP 800-50, SP 800-53).**

Yes

Section 4: Security Training

Comments: FISMA Report: Finding No. 4, Issue 4 - The OCIO Needs to Improve New User Security Training.
EDUCATE Report: Finding No. 13, Documentation of Security Awareness Training Needed Improvement.

4.b(8). **Identification and tracking of the status of specialized training for personnel (including employees, contractors, and other Agency users) with significant information security responsibilities is not adequate in accordance with government policies (SP 800-50, SP 800-53).**

No

Comments: No exceptions noted.

4.b(9). **Training content for individuals with significant information security responsibilities is not adequate in accordance with government policies (SP 800-53, SP 800-16).**

No

Comments: No exceptions noted.

4.b(10). **Less than 90% of personnel (including employees, contractors, and other agency users) with access privileges completed security awareness training in the past year.**

No

Comments: No exceptions noted.

4.b(11). **Less than 90% of employees, contractors, and other users with significant security responsibilities completed specialized security awareness training in the past year.**

No

Comments: No exceptions noted.

4.b(12). **Other**

No

Comments: No exceptions noted.

Section 5: POA&M

5.b. **The Agency has established and is maintaining a POA&M program that tracks and remediates known information security weaknesses. However, the Agency needs to make significant improvements as noted below.**

5.b. **The Agency has established and is maintaining a POA&M program that tracks and remediates known information security weaknesses. However, the Agency needs to make significant improvements as noted below.**

Section 5: POA&M

5.b(1). **POA&M Policy is not fully developed.**

No

Comments: No exceptions noted.

5.b(2). **POA&M procedures are not fully developed and sufficiently detailed.**

Yes

Comments: EDUCATE Report: Finding No. 14, Plan of Action and Milestones Process was not Adequately Managed.

5.b(3). **POA&M procedures are not consistently implemented in accordance with government policies.**

Yes

Comments: EDUCATE Report: Finding No. 14, Plan of Action and Milestones Process was not Adequately Managed.

5.b(4). **POA&Ms do not include security weaknesses discovered during assessments of security controls and requiring remediation. (OMB M-04-25).**

Yes

Comments: EDUCATE Report: Finding No. 14, Plan of Action and Milestones Process was not Adequately Managed.

5.b(5). **Remediation actions do not sufficiently address weaknesses in accordance with government policies (NIST SP 800-53, Rev. 3, Sect. 3.4 Monitoring Security Controls).**

No

Comments: No exceptions noted.

5.b(6). **Source of security weaknesses are not tracked (OMB M-04-25).**

No

Comments: No exceptions noted.

5.b(7). **Security weaknesses are not appropriately prioritized (OMB M-04-25).**

No

Comments: No exceptions noted.

5.b(8). **Milestone dates are not adhered to. (OMB M-04-25).**

No

Section 5: POA&M

Comments: No exceptions noted.

5.b(9). **Initial target remediation dates are frequently missed (OMB M-04-25).**

No

Comments: No exceptions noted.

5.b(10). **POA&Ms are not updated in a timely manner (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).**

No

Comments: No exceptions noted.

5.b(11). **Costs associated with remediating weaknesses are not identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25).**

No

Comments: No exceptions noted.

5.b(12). **Agency CIO does not track and review POA&Ms (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).**

No

Comments: No exceptions noted.

5.b(13). **Other**

No

Comments: No exceptions noted.

Section 6: Remote Access Management

6.b. **The Agency has established and is maintaining a remote access program. However, the Agency needs to make significant improvements as noted below.**

6.b(1). **Remote access policy is not fully developed (NIST 800-53: AC-1, AC-17).**

Yes

Comments: FISMA Report: Finding No. 6, Remote Access Management, Issue 6a, Remote Access Policy Needs Improvement.

6.b(2). **Remote access procedures are not fully developed and sufficiently detailed (NIST 800-53: AC-1, AC-17).**

Yes

Comments: FISMA Report: Finding No. 6, Remote Access Management, Issue 6a, Remote Access Policy Needs Improvement.

6.b(3). **Remote access procedures are not consistently implemented in accordance with government policies (NIST 800-53: AC-1, AC-17).**

Yes

Comments: FISMA Report: Finding No. 6, Remote Access Management, Issue 6a, Remote Access Policy Needs Improvement.
FISMA Report: Finding No. 6, Issue 6b, Remote Access Controls, Settings and Automated Restrictions Need Improvement.

6.b(4). **Telecommuting policy is not fully developed (NIST 800-46, Section 5.1).**

Yes

Comments: FISMA Report: Finding No. 6, Remote Access Management, Issue 6a, Remote Access Policy Needs Improvement.

6.b(5). **Telecommuting procedures are not fully developed or sufficiently detailed in accordance with government policies (NIST 800-46, Section 5.4).**

Yes

Comments: FISMA Report: Finding No. 6, Remote Access Management, Issue 6a, Remote Access Policy Needs Improvement.
FISMA Report: Finding No. 6, Issue 6b, Remote Access Controls, Settings and Automated Restrictions Need Improvement.

6.b(6). **Agency cannot identify all users who require remote access (NIST 800-46, Section 4.2, Section 5.1).**

No

Comments: No exceptions noted.

6.b(7). **6.b(7). Multi-factor authentication is not properly deployed (NIST 800-46, Section 2.2, Section 3.3).**

Yes

Section 6: Remote Access Management

Comments: FISMA Report: Finding No. 6, Remote Access Management, Issue 6c, Two-Factor Authentication Not Fully Implemented.
EDUCATE Report: Finding No. 4, Remote Access Software Was Not Compliant with OMB and NIST Standards.

6.b(8). **Agency has not identified all remote devices (NIST 800-46, Section 2.1).**

No

Comments: No exceptions noted.

6.b(9). **Agency has not determined all remote devices and/or end user computers have been properly secured (NIST 800-46, Section 3.1 and 4.2).**

Yes

Comments: FISMA Report: Finding No. 6, Remote Access Management, Issue 6b – Remote Access Controls, Settings and Automated Restrictions Need Improvement.
EDUCATE Report: Finding No. 4, Remote Access Software Was Not Compliant with OMB and NIST Standards.

6.b(10). **Agency does not adequately monitor remote devices when connected to the Agency's networks remotely in accordance with government policies (NIST 800-46, Section 3.2).**

Yes

Comments: FISMA Report: Finding No. 6, Remote Access Management, Issue 6b – Remote Access Controls, Settings and Automated Restrictions Need Improvement.

6.b(11). **Lost or stolen devices are not disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines).**

No

Comments: No exceptions noted.

6.b(12). **Remote access rules of behavior are not adequate in accordance with government policies (NIST 800-53, PL-4).**

No

6.b(13). **Remote access user agreements are not adequate in accordance with government policies (NIST 800-46, Section 5.1, NIST 800-53, PS-6).**

No

Section 6: Remote Access Management

Comments: No exceptions noted.

6.b(14). **Other**

No

Comments: No exceptions noted.

Section 7: Identity and Access Management

7.b. **The Agency has established and is maintaining an identity and access management program that identifies users and network devices. However, the Agency needs to make significant improvements as noted below.**

7.b(1). **Account management policy is not fully developed (NIST 800-53: AC-1).**

No

Comments: No exceptions noted.

7.b(2). **Account management procedures are not fully developed and sufficiently detailed (NIST 800-53: AC-1).**

Yes

Comments: FISMA Report: Finding No. 7, Identity and Access Management, Issue 7 - The Identity and Access Management Program Needs Improvement.

7.b(3). **Account management procedures are not consistently implemented in accordance with government policies (NIST 800-53: AC-2).**

Yes

Comments: FISMA Report: Finding No. 7, Identity and Access Management, Issue 7 - The Identity and Access Management Program Needs Improvement.
EDUCATE Report: Finding No. 5, Controls for Identifying and Resolving Vulnerabilities Needed Improvement.
EDUCATE Report: Finding No. 7, Account and Identity Management Process Required Significant Improvement.

7.b(4). **Agency cannot identify all User and Non-User Accounts (NIST 800-53, AC-2).**

No

Comments: No exceptions noted.

7.b(5). **Accounts are not properly issued to new users (NIST 800-53, AC-2).**

No

Comments: No exceptions noted.

7.b(6). **Accounts are not properly terminated when users no longer require access (NIST 800-53, AC-2).**

Yes

Comments: EDUCATE Report: Finding No. 7, Account and Identity Management Process Required Significant Improvement.

7.b(7). **Agency does not use multi-factor authentication where required (NIST 800-53, IA-2).**

Yes

Comments: FISMA Report: Finding No. 6, Remote Access Management, Issue 6c, Two-Factor Authentication Not Fully Implemented.
EDUCATE Report: Finding No. 7, Account and Identity Management Process Required Significant Improvement.

7.b(8). **Agency has not 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: FISMA Report: Finding No. 6, Remote Access Management, Issue 6c, Two-Factor Authentication Not Fully Implemented.
EDUCATE Report: Finding No. 7, Account and Identity Management Process Required Significant Improvement.

7.b(9). **Privileges granted are excessive or result in capability to perform conflicting functions (NIST 800-53, AC-2, AC-6).**

No

Comments: No exceptions noted.

7.b(10). **Agency does not use dual accounts for administrators (NIST 800-53, AC-5, AC-6).**

No

Comments: No exceptions noted.

7.b(11). **Network devices are not properly authenticated (NIST 800-53, IA-3).**

No

Comments: No exceptions noted.

7.b(12). **The process for requesting or approving membership in shared privileged accounts is not adequate in accordance to government policies.**

Section 7: Identity and Access Management

No

Comments: No exceptions noted.

7.b(13). **Use of shared privileged accounts is not necessary or justified.**

No

Comments: No exceptions noted.

7.b(14). **When shared accounts are used, the Agency does not renew shared account credentials when a member leaves the group.**

No

Comments: No exceptions noted.

7.b(15). **Other**

No

Comments: No exceptions noted.

Section 8: Continuous Monitoring Management

8.b. **The Agency has established an enterprise-wide continuous monitoring program that assesses the security state of information systems. However, the Agency needs to make significant improvements as noted below.**

8.b(1). **Continuous monitoring policy is not fully developed (NIST 800-53: CA-7).**

Yes

Comments: FISMA Report: Finding No. 1, Risk Management, Issue 1a, OCIO Needs to Fully Implement the Risk Management Program.
EDUCATE Report: Finding No. 12, Department Needed to Establish an Organization-Wide Risk Management Strategy.

8.b(2). **Continuous monitoring procedures are not fully developed (NIST 800-53: CA-7).**

Yes

Comments: FISMA Report: Finding No. 1, Risk Management, Issue 1a, OCIO Needs to Fully Implement the Risk Management Program.
EDUCATE Report: Finding No. 12, Department Needed to Establish an Organization-Wide Risk Management Strategy.

Section 8: Continuous Monitoring Management

8.b(3). **Continuous monitoring procedures are not consistently implemented (NIST 800-53: CA-7; 800-37 Rev 1, Appendix G).**

Yes

Comments: FISMA Report: Finding No. 1, Risk Management, Issue 1a, OCIO Needs to Fully Implement the Risk Management Program.
EDUCATE Report: Finding No. 12, Department Needed to Establish an Organization-Wide Risk Management Strategy.

8.b(4). **Strategy or plan has not been fully developed for enterprise-wide continuous monitoring (NIST 800-37 Rev 1, Appendix G).**

Yes

Comments: FISMA Report: Finding No. 1, Risk Management, Issue 1a, OCIO Needs to Fully Implement the Risk Management Program.
EDUCATE Report: Finding No. 12, Department Needed to Establish an Organization- Wide Risk Management Strategy.

8.b(5). **Ongoing assessments of security controls (system-specific, hybrid, and common) have not been performed (NIST 800-53, NIST 800-53A).**

Yes

Comments: FISMA Report: Finding No. 1, Risk Management, Issue 1a, OCIO Needs to Fully Implement the Risk Management Program.
EDUCATE Report: Finding No. 12, Department Needed to Establish an Organization-Wide Risk Management Strategy.

8.b(6). **The following were not provided to the authorizing official or other key system officials: security status reports covering continuous monitoring results, updates to security plans, security assessment reports, and POA&Ms (NIST 800-53, NIST 800-53A).**

No

Comments: No exceptions noted.

8.b(7). **Other**

No

Comments: No exceptions noted.

Section 9: Contingency Planning

Section 9: Contingency Planning

9.b. **The Agency has established and is maintaining an enterprise-wide business continuity/disaster recovery program. However, the Agency needs to make significant improvements as noted below.**

9.b(1). **Contingency planning policy is not fully developed contingency planning policy is not consistently implemented (NIST 800-53: CP-1).**

No

Comments: No exceptions noted.

9.b(2). **Contingency planning procedures are not fully developed (NIST 800-53: CP-1).**

Yes

Comments: FISMA Report: Finding No. 8, Issue 8, Contingency Planning Needs Improvement.

9.b(3). **Contingency planning procedures are not consistently implemented (NIST 800-53; 800-34).**

Yes

Comments: FISMA Report: Finding No. 8, Issue 8, Contingency Planning Needs Improvement.

9.b(4). **An overall business impact assessment has not been performed (NIST SP 800-34).**

Yes

Comments: EDUCATE Report: Finding No. 11, Contingency Planning Program Needed Improvement.

9.b(5). **Development of organization, component, or infrastructure recovery strategies and plans has not been accomplished (NIST SP 800-34).**

No

Comments: No exceptions noted.

9.b(6). **A business continuity/disaster recovery plan has not been developed (FCD1, NIST SP 800-34).**

No

Comments: No exceptions noted.

9.b(7). **A business continuity/disaster recovery plan has been developed, but not fully implemented (FCD1, NIST SP 800-34).**

Yes

Comments: EDUCATE Report: Finding No.11, Contingency Planning Program Needed Improvement.

9.b(8). **System contingency plans missing or incomplete (FCD1, NIST SP 800-34, NIST SP 800-53).**

Yes

Comments: FISMA Report: Finding No. 8, Issue 8, Contingency Planning Needs Improvement.
EDUCATE Report: Finding No. 11, Contingency Planning Program Needed Improvement.

9.b(9). **Systems contingency plans are not tested (FCD1, NIST SP 800-34, NIST SP 800-53).**

No

Comments: No exceptions noted.

9.b(10). **Test, training, and exercise programs have not been developed (FCD1, NIST SP 800-34, NIST 800-53).**

No

Comments: No exceptions noted.

9.b(11). **Test, training, and exercise programs have been developed, but are not fully implemented (FCD1, NIST SP 800-34, NIST SP 800-53).**

No

Comments: No exceptions noted.

9.b(12). **After-action report did not address issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34).**

No

Comments: No exceptions noted.

9.b(13). **Systems do not have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).**

No

Comments: No exceptions noted.

9.b(14). **Alternate processing sites are subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).**

No

Comments: No exceptions noted.

9.b(15). **Backups of information are not performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).**

No

Comments: No exceptions noted.

Section 9: Contingency Planning

9.b(16). **Backups are not appropriately tested (FCD1, NIST SP 800-34, NIST SP 800-53).**

No

Comments: No exceptions noted.

9.b(17). **Backups are not properly secured and protected (FCD1, NIST SP 800-34, NIST SP 800-53).**

No

Comments: No exceptions noted.

9.b(18). **Contingency planning does not consider supply chain threats.**

No

Comments: No exceptions noted.

9.b(19). **Other**

No

Comments: No exceptions noted.

Section 10: Contractor Systems

10.b. **The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in public cloud. However, the Agency needs to make significant improvements as noted below.**

10.b(1). **Policies to oversee systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud, are not fully developed.**

No

Comments: No exceptions noted.

10.b(2). **Procedures to oversee systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud, are not fully developed.**

Yes

Comments: FISMA Report: Finding No. 9, Issue 9, Contract Monitoring Controls Need Improvement.

10.b(3). **Procedures to oversee systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud are not consistently implemented.**

Section 10: Contractor Systems

Yes

Comments: FISMA Report: Finding No. 9, Issue 9, Contract Monitoring Controls Need Improvement.

10.b(4). **The inventory of systems owned or operated by contractors or other entities, including Agency systems and services residing in public cloud, is not complete in accordance with government policies (NIST 800-53: PM-5).**

No

Comments: No exceptions noted.

10.b(5). **The inventory does not identify interfaces between contractor/entity-operated systems to Agency owned and operated systems.**

Yes

Comments: EDUCATE Report: Finding No. 8, Ensure All Connecting Systems Are Compliant with Federal Information Security Requirements.

10.b(6). **The inventory of contractor/entity-operated systems, including interfaces, is not updated at least annually.**

No

Comments: No exceptions noted.

10.b(7). **Systems owned or operated by contractors and entities are not subject to NIST and OMB's FISMA requirements (e.g., security requirements).**

No

Comments: No exceptions noted.

10.b(8). **Systems owned or operated by contractor's and entities do not meet NIST and OMB's FISMA requirements (e.g., security requirements).**

Yes

Section 10: Contractor Systems

Comments:

FISMA Report: Finding No. 1, Issue 1a, OCIO Needs to Fully Implement the Risk Management Program, and Issue 1b, The OCIO Needs to Improve the System Authorization Process. Finding No. 2, Issue 2a, Patch Management Program Needs Improvement, and Issue 2b, Access Switch Port Security Needs Improvement. Finding No. 4, Issue 4, The OCIO Needs to Improve New User Security Training. Finding No. 6, Issue 6a, Remote Access Policy Needs Improvement, Issue 6b, Remote Access Controls, Settings and Automated Restrictions Need Improvement, and Issue 6c, Two-Factor Authentication Not Fully Implemented. Finding No. 7, Issue 7, The Identity and Access Management Program Needs Improvement. FISMA Report: Finding No. 8, Issue 8, Contingency Planning Needs Improvement.

IPAR: “Incident Response and Reporting Procedures” Finding No. 1, The Department has not Detected, Reported, or Responded Appropriately to Security Incidents.

10.b(9). Interface agreements (e.g., MOUs) are not properly documented, authorized, or maintained.

Yes

Comments:

EDUCATE Report: Finding No. 8, Ensure All Connecting Systems Are Compliant with Federal Information Security Requirements.

10.b(10). Other

No

Comments:

Continued from 10.b(8)

EDUCATE Report: Finding No. 1, Security Configuration Management Process, Finding No. 2, Network Security Controls over Hardware Devices and Software, Finding No. 3, Security Patch Management Process, Finding No. 4, Remote Access Software Was Not Compliant, Finding No. 5, Controls for Identifying and Resolving Vulnerabilities, Finding No. 6, Incident Response Program Needed Improvement, Finding No. 7, Account and Identity Management Process Required Significant Improvement, Finding No. 8, EDNIS Security Plan and Interconnections, Finding No. 9, FDCC Security Configuration Management Process Needed Improvement, Finding No. 10, Security Assessment and Authorization Documents, Finding No.11, Contingency Planning Program Needed Improvement, Finding No. 12, Organization-Wide Risk Management Strategy Needed to Be Established, Finding No. 13. Documentation of Security Awareness Training, and Finding No. 14, Plan of Action and Milestones Process.

Section 11: Security Capital Planning

11.a. The Agency has established and maintains a security capital planning and investment program for information security. Although

improvement opportunities may have been identified by the OIG, the program includes the following attributes:

11.a(1). **Documented policies and procedures to address information security in the capital planning and investment control process.**

No

Comments: FISMA Report: Finding No. 10, Issue 10, Security Capital Planning Needs Improvement.

11.a(2). **Includes information security requirements as part of the capital planning and investment process.**

No

Comments: FISMA Report: Finding No. 10, Issue 10, Security Capital Planning Needs Improvement.

11.a(3). **Establishes a discrete line item for information security in organizational programming and documentation.**

Yes

Comments: No exceptions noted.

11.a(4). **Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required.**

Yes

Comments: No exceptions noted.

11.a(5). **Ensures that information security resources are available for expenditure as planned.**

Yes

Comments: No exceptions noted.

Enclosure 2: Criteria

"Homeland Security Presidential Directive/HSPD-12," dated 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," dated August 5, 2005

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

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

OMB M-10-15, "FY 2010 Reporting Instructions for the Federal Information Security Management Act (FISMA) and Agency Privacy Management," dated April 21, 2010

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

OMB Circular A-11, "Preparation, Submission and Execution of the Budget," dated June 2008, Section 53—Information Technology and E-Government and Section 300—Planning, Budgeting, Acquisition, and Management of Capital Assets

OMB Circular A-123, "Management's Responsibility for Internal Control," dated 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," dated February 2004

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

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

Federal Register 06-14-2004 United States Office of Personnel Management (OPM) 5 CFR 930 "IS Security Awareness Training," dated June 14, 2004

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

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

NIST SP 800-46, Revision 1, “Guide for Assessing the Security Controls in Federal Information Systems and Organizations,” dated June 2010

NIST SP 800-53, Revision 3, “Recommended Security Controls for Federal Info Systems & Organizations,” dated August 2009

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

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

NIST SP 800-123, “Guide to General Server Security,” dated July 2008

NIST SP 800-128, “Guide for Security Configuration Management Information Systems,” dated March 2010

Office of the Chief Information Officer (OCIO) -01, “Handbook for Information Assurance (IA) Policy, “ dated March 31, 2006

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

OCIO -10, “Handbook for Information Technology Security Contingency Planning Procedures,” dated July 12, 2005

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

UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF THE CHIEF INFORMATION OFFICER

THE CHIEF INFORMATION OFFICER

MEMORANDUM

DATE: October 12, 2011

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

FROM: Danny A. Harris, Ph.D.

SUBJECT: Draft Audit Report
Audit of the U.S. Department of Education's Compliance with the Federal Infonnation Security Management Act for Fiscal Year 2011 Control Number ED-OIG/A11L0003

Thank you for the opportunity to review and comment on the draft Office of Inspector General's (OIG) report, Audit of the U.S. Department of Education's Compliance with the Federal Information Security Management Act (FISMA) for Fiscal Year 2011, Control Number ED-OIG/A11L0003. The Department sincerely values the FISMA audit activity conducted this year by OIG and appreciates the benefits of the collaborative relationship between OIG and the Department, formed through years of partnering and the sharing of mutual goals and objectives.

The results of the FISMA audit clearly indicate that the Department continues to show incremental and credible improvement in meeting the requirements of the FISMA. While the Office of the Chief Infonnation Officer (OCIO) agrees with many of the findings and recommendations arising from this audit, we believe that the methodology used to conduct this audit limited OIG's ability to produce a fair and balanced report. Specifically, (1) the timing of the audit did not allow OIG to acknowledge the Department's final set of achievements for the 2011 fiscal year; (2) throughout the report OIG references system-specific findings from previously issued OIG reports, but fails to mention that these findings have since been resolved by the Department; and, (3) several recommended actions were already under way at the time of OIG's review, and, as noted below, some were completed before the first draft review was provided to management.

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

Risk Management

The Department appreciates OIG's recognition that "OCIO took a number of proactive steps to build and develop the Department's risk management function." OIG recommends that the Department enhance its continuous system authorization and continuous monitoring procedures to ensure that security controls are monitored on an ongoing basis. The Department concurs. OCIO Information Assurance Services (IAS) has allocated Fiscal Year (FY) 2012 funding to purchase and implement the iPost risk scoring tool, which will allow the Department to continuously monitor and report risks on the Department's Information Technology infrastructure. Additionally, IAS is in the process of redesigning business processes that will allow system owners to continuously monitor technical security controls using Security Content Automation Protocol (SCAP) compliant tools, such as Red Seal, Big Fix, and Triumfant.

Page 7 of the report inaccurately states that the Federal Information Processing Standards (FIPS) 199 level in the Education's Security Tracking and Reporting System (EDSTAR) system security plan (SSP) did not match the FIPS 199 level in the FISMA FY 2011 Inventory (as of June 30, 2011). The Operational Vulnerability Management Solution (OVMS) categorizes EDSTAR as having a FIPS risk impact of "High." Additionally, the EDSTAR SSP (uploaded to OVMS on October 8, 2010) identifies this system as high.

Page 8 references previous audits "IT Security Controls over the Debt Management Collection Process, Phase II, Fiscal Year 2008" and "Security over Certification and Accreditation for Information Systems" in which similar security authorization issues were identified by OIG. However, the report fails to include the corrective action taken by Federal Student Aid (FSA) to remediate the issues noted in these prior reports. FSA implemented continuous security authorization (CSA) to address the deficiencies noted in these audit reports and to improve their certification and accreditation (C&A) program. FSA has enrolled thirteen of its systems into the process; enrollment into CSA occurs only after a system completes a current Security Authorization that has baselined its controls for continued scheduled testing and monitoring in accordance with National Institute of Standards and Technology (NIST) requirements. The CSA process has been reviewed to the Department's Chief Information Security Officer (CISO) and is in the final stages of being formalized by FSA support contractors.

Page 9 of the report inaccurately states, "Neither the EINSTEIN nor the Managed Security Service Provider (MSSP) intrusion detection systems had an Memorandum of Understanding (MOU)." Attachment A provides a copy of the service level agreement that was entered into by the Department and the Department of Homeland Security (DHS) on June 9, 2011. Attachment B provides a copy of the MOU that was entered into by the Department's MSSP, Federal Aviation Administration and the Department on August 9, 2010. Also the Department of Justice Cyber Security Assessment and Management, noted by OIG as not having an up to date MOU, was decommissioned in April 2010.

OIG Recommendation 1.1 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 the Office of Management and Budget and NIST.

Management Response: OCIO concurs with this recommendation. OCIO will revise OCIO-01, "Handbook for Information Assurance Security Policy," and OCIO-05, "Handbook for Information Technology Security Certification and Accreditation Procedures," to include a comprehensive governance structure and organization-wide risk management strategy that includes the techniques and methodologies that the Department will employ to assess information systems related risk to preserve availability, confidentiality, and integrity.

The risk management program will be implemented to manage threats and vulnerabilities with continuous monitoring to determine effectiveness, and to calculate more accurately the estimated residual risk with sustaining computer and network security measures that meet changing business requirements without negatively impacting the business viability. These revisions will be completed by August 30, 2012.

OIG Recommendation 1.2 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.)

Management Response: OCIO concurs with this recommendation. OCIO IAS will revise OCIO-05, "Handbook for Information Technology Security Certification and Accreditation Procedures," to require that all system authorization documentation be uploaded to OVMS to ensure it is readily available. This requirement will be communicated to Department Information System Security Officers (ISSO) during the second quarter ISSO meeting.

OCIO IAS will work with the responsible ISSOs to resolve the deficiencies noted in Issue 1b by April 1, 2012.

OIG Recommendation 1.3 Ensure that system authorizations are completed at least every 3 years, when there are significant changes to the systems, or 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.

Management Response: OCIO concurs with this recommendation. As noted in the response memorandum titled "Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) Information Security Audit Control Number ED-OIG/AI 1L0001," OCIO IAS is working with OVMS developers to create enhancements that will allow for the automated tracking of Department systems reaccreditation and recertification. This enhancement is scheduled to be completed by August 30, 2012.

OCIO has established a tiger team to assess the information systems that have been identified as having outstanding or incomplete C&A packages. The team shall gather all supporting evidence and documentation, and develop the required documents to resolve the deficiencies noted in Issue 1b by April 1, 2012.

OCIO will revise OCIO-05, "Handbook for Information Technology Security Certification and Accreditation Procedures," to standardize the enterprise-wide layered inherited IA controls, the C&A process and resolve the lack of cohesiveness within the different certification packages, along with implementing a continuous monitoring phase ensuring configuration management changes are approved and properly recorded within OVMS. The revisions will be completed by August 30, 2012.

OIG Recommendation 1.4 Develop controls to ensure timely re-authorizations for systems, avoiding gaps in ATO coverage.

Management Response: OCIO concurs with this recommendation. As previously mentioned, OCIO IAS has budgeted in FY12 and FY13 to implement automated continuous security authorization in accordance with NIST and DHS guidance by December 30, 2012.

OIG Recommendation 1.5 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.

Management Response: OCIO concurs with this recommendation. OCIO will revise OCIO-01, "Handbook for Information Assurance Security Policy," and OCIO-05, "Handbook for Information Technology Security Certification and Accreditation Procedures," to be in compliance with OMB and NIST guidance pertaining to continuous system authorization and continuous monitoring, and interim authority to operate for security authorizations. The revisions will be completed by August 30, 2012.

Configuration Management

Page 12 inaccurately states, "OCIO was not aware that Perot Systems had not installed security patches on all network devices within the timeframe required by Dell's process (30 days)." The Department receives a monthly report of non-installed patches from Dell, see enclosure.

OIG Recommendation 2.1 Develop, approve, and implement an enterprise-wide patch management policy that complies with OMB, NIST, and other applicable Federal guidelines.

Management Response: OCIO concurs with this recommendation. The Department will revise the Vulnerability and Patch Management Guidance to comply with OMB, NIST, and other applicable Federal guidelines. The Patch Management Guidance will be revised by October 31, 2011.

OIG Recommendation 2.2 Circulate and distribute the final approved patch management policy to all principal offices and contractors for consistent implementation.

Management Response: OCIO concurs with this recommendation. The finalized Vulnerability and Patch Management Guidance will be distributed to all principal offices and contractors by December 1, 2011.

OIG Recommendation 2.3 Require the 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.

Management Response: OCIO concurs with this recommendation. OCIO IAS is in the process of developing security configuration baselines for all Department devices, including switches, which will incorporate best practices from NIST and DISA network security checklists and other related guidance. The Department is also implementing the RedSeal change detection tool, using configuration files from EDUCATE and FSA's Virtual Data Center (VDC). This tool will be utilized to monitor for compliance with the Department's baseline configuration guidelines. As the RedSeal project evolves, it will become one of the centerpieces of the Continuous Monitoring Program through tracking and approving changes to the network devices designed to resolve network security configuration vulnerabilities and ensuring compliance to baseline security configurations. Red Seal will be fully deployed by January 15, 2012.

It is important to note that in order to exploit the switch port security vulnerability described in the report, a perpetrator must have physical access, which would require the circumvention of two increasingly restrictive physical layers of defense, using an unauthorized badge. The only way a person without foreknowledge could have discovered the existence of this particular vulnerability would be to scan the network.

OIG Recommendation 2.4 Require the contractor to shutdown or disable unassigned/unused switch port connections throughout the enterprise.

Management Response: OCIO partially concurs with this recommendation. The Department CISO will issue a memorandum directing Dell to submit Risk Acceptance Forms (RAF) for unassigned/unused switch port connections on the Department's network by October 21, 2011. These RAFs will be submitted to the CISO for approval.

Security Training

OIG Recommendation 4.1 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.

Management Response: OCIO concurs with this recommendation. OCIO will develop a new user IT security awareness and training course for new employees that will be provided through the Department's Corporate Onboarding Process, EDStart. Employees will be provided new user training material through EDStart on-line. This new procedure will be implemented by December 30, 2011.

OIG Recommendation 4.2 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.

Management Response: OCIO concurs with this recommendation. OCIO will revise IT security awareness and training program policies and procedures to require that new hire IT security awareness training be completed prior to access to the Department's network or any Departmental information systems. The revised policy will be published by December 30, 2011.

Remote Access Management

The Department does not agree with OIG's statement that Two-Factor Authentication (TFA) has not been implemented. On August 31, 2011, the Department completed a project that required employees and contractors to use Personal Identity Verification cards to obtain access to the Department's network. On September 19, 2011, the Department went into a disaster recovery mode that temporarily allowed the use of username and password.

The Department currently requires TFA for FSA users and has current plans to require TFA for all employees and contractors. On May 17, 2011, FSA made TFA mandatory for employees accessing the FSA version of Citrix remotely. On October 25, 2011, the rest of the Department will be required to use TFA when remotely connecting to the ED.gov version of Citrix.

FSA has initiated a pilot with seven foreign schools and is in the process of implementing TFA at certain pre-identified CONUS schools. FSA anticipates full implementation of TFA for all external partners by September 30, 2012.

OIG Recommendation 6.1 Develop policy and procedures that clearly define telework security and remote access requirements; types of remote access the organization permits; which types of devices are permitted to use each form of remote access; the type of access each type of teleworker is granted; how the remote access servers are to be administered; and how (automated) policies in those servers are to be updated.

Management Response: OCIO concurs with this recommendation. OCIO IAS will develop a telework security policy to clearly define the Department's remote access requirements, types of remote access permitted, which types of devices are permitted to use each form of remote access, the type of access each type of teleworker is granted, how the remote access servers are to be administered, and how (automated) policies in those servers are to be updated, in accordance with NIST SP 800-46, Revision 1, "Guide to Enterprise Telework and Remote Access Security." The policy will be published by May 1, 2012.

OIG Recommendation 6.2 Implement an automated enforcement or endpoint/media encryption solution that will automatically encrypt all information saved to external devices.

Management Response: OCIO concurs with this recommendation. OCIO IAS is in the process of testing a lightweight portable security (LPS) remote access solution that can be customized to automatically encrypt all information saved to external devices. Testing will be completed by December 30, 2012.

OIG Recommendation 6.3 Configure all remote sessions to time-out after 30 minutes of inactivity as mandated by OMB.

Management Response: OCIO concurs with this recommendation. On September 16, 2011, IAS submitted a request to Dell to modify the current sixty minute timeout value on Citrix and FirePass to thirty minutes. This change will be effective on October 17, 2011.

OIG Recommendation 6.4 Configure the new Citrix 2008 servers to log connectivity activity and review these logs for indications of attacks or anomalies.

Management Response: OCIO concurs with this recommendation. The Department CISO will issue a memorandum directing Dell to configure all Citrix 2008 servers to log connectivity activity and review these logs for indications of attacks or anomalies by October 18, 2011.

OIG Recommendation 6.5 Configure the EDUCATE Citrix to allow mapping only to GFE devices.

Management Response: OCIO does not concur with this recommendation. Configuring CITRIX to map only to GFE without additional architectural changes will impede mission critical functions and the ability to implement telework in accordance with OMB guidance. OCIO has implemented two factor authentication for the EDUCATE CITRIX capability and is working on additional architectural changes to enhance the security capability and policy for remote access.

As previously mentioned, OCIO IAS is in the process of reviewing alternatives for a Virtual Government Furnished Equipment solution for untrusted hardware. OCIO IAS is working with the Department of Defense on a LPS bootable CD-ROM solution that will work with the EDUCATE Citrix infrastructure to ensure the Department's security protocols are fully implemented on non-GFE. IAS has received the prototype and plans to test this solution.

Identity and Access Management

As noted in the response memorandum titled, "Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) Information Security Audit Control Number ED-OIG/A11L0001," the Department has taken several steps to strengthen logical access controls. The Department has implemented an automated process in which a weekly report is generated to identify user objects for removal that were inactive for longer than 90 days within the EDUCATE ED.GOV AD Domain environment. On August 18, 2011, the Department issued notification to Dell Systems that the 272 active directory accounts identified as having password settings of "Do Not Expire" be disabled.

OIG Recommendation 7.1 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, OMB, and NIST guidance.

Management Response: OCIO concurs with this recommendation. In September 2011, IAS awarded the enterprise security architecture task order. A key deliverable under this task order is an engineering study on the implementation and life cycle support required for the integration and operation of Network Access Control (NAC). The implementation of a NAC device on the network would allow the Department to (1) identify all devices that are attached to the network; (2) distinguish the devices from users; and, (3) authenticate devices that are connected to the network consistent with FISMA, OMB, and NIST guidance.

The OCIO IAS Policy Team will use the results from this study to establish identity and access management procedures by April 1, 2012.

Contingency Planning

Page 21 states, "In an October 2009 report, the OIG reported findings regarding the contingency planning process for CPS, NSLDS, and VDC." FSA completed the Business Impact Analysis (BIA) for Central Processing System in April 2011 and is in the final stages of completing the contingency plan (CP). FSA completed revisions to the BIA and CP documents for National Student Loan Database System in November 2010. The VDC facility is represented in the overall Business Impact Analysis which is contained in Appendix K of the Department's Continuity of Services Plan.

FSA has made significant progress during 2011 to address VDC application specific security documentation deficiencies. The COOP Plan has been published and is managed at the Department level. As of September 30, 2011, the FSA VDC Continuity of Services Plan contains Appendix N: Virtual Private Network (VPN) Tunnel. These alternate VPN tunnels are available to support external partner connectivity to the Philadelphia SunGard site in the case of an actual disaster recovery event impacting the Plano Technology Center. These connections are configured to utilize Dell Services managed infrastructure at the Dell Services data center in Florence, Kentucky.

Page 21 states, "FSA did not request telecommunication service priority (TSP) for national security emergency preparedness and did not include TSP requirements in the VDC Telecommunications Plan." FSA closed this prior year FISMA finding in March 2011 by updating the contents of the VDC Telecommunications Plan to include the criteria for Telecommunication Service Provider (TSP) codes, as well as submitting TSP code requests to OCIO and Office of Management (OM) for all related circuits.

Page 22 states, "The OCIO had not requested TSP codes for National Security Emergency Preparedness as required by the Department of Homeland Security. These codes are necessary to pennit the resumption of infonnation system operations for essential missions and business functions when the primary telecommunications capabilities are unavailable." As noted in the response memorandum titled, "Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) Information Security Audit Control Number ED-OIG/A11L0001", OCIO Information Technology Services (ITS) has solicited price quotes for TSP restoration services for EDUCATE supported circuits. FSA has submitted DHS provided TSP Request Forms to OM Security Services division for processing. OCIO ITS plans to have the required procedures and process implemented by March 1, 2012.

OIG Recommendation 8.1 We recommend that the OCIO review and update system contingency plans for the nine systems (list provided to the OCIO) to ensure that all the required contingency planning elements are included as required by NIST guidance.

Management Response: OCIO concurs with this recommendation. The CP deficiencies noted by the FISMA audit team have been submitted to the responsible system owners for revision. The updates to the contingency plans for the nine systems in question will be completed by March 31, 2012.

In addition, the OCIO IAS division has established a Policy Team to revise the Department's security guidelines, templates, procedures, handbooks, and supporting documentation, including the Contingency Plan Template, to ensure the Department's compliance with current NIST guidance.

Physical Security Deficiency 2

The deficiency noted in the main distribution frame room was resolved on October 7, 2011.

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

Requests for copies of Attachments A & B to the Department's comments, should be directed to:

U.S. Department of Education
Office of Management
Regulatory Information Management Services
400 Maryland Avenue, SW, LBJ 2W220
Washington, DC 20202-4536
ATTN: FOIA Public Liaison

http://www2.ed.gov/policy/gen/leg/foia/request_foia.html