




UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Information Technology Audit Division

September 5, 2012

Memorandum

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

SUBJECT: Final Audit Report Reissuance
Education Department Utility for Communications, Applications, and Technology
Environment (EDUCATE) Information Security Audit
Control Number ED-OIG/A11L0001

The attached final audit report, originally issued on September 30, 2011, was reissued and included changes to (1) the report cover page, (2) the inside cover notice, and (3) my final report transmittal memorandum to Danny A. Harris, Ph.D., Chief Information Officer. The intent of these revisions is to demonstrate a clear understanding that Williams, Adley & Company-DC, LLC, was responsible for the attached auditor's report and the conclusions expressed therein.

Although this is a reissuance of an existing report, the changes cited above do not impact any of the findings and recommendations contained in the September 30, 2011 report. Also, this reissuance does not require adjustments to any corrective action completion dates being monitored and tracked through the Department's Audit Accountability and Resolution Tracking System. In addition, because the reissuance does not impact the content of the audit report, September 30, 2011, will remain as the official issue date and does not affect the Office of Inspector General's Semiannual Report to Congress reporting requirements.

REPORT OF THE INDEPENDENT AUDITORS

Final Report

**Education Department Utility for
Communications, Applications, and
Technology Environment (EDUCATE)
Information Security Audit
ED-OIG/A11L0001**



**Prepared by:
Williams, Adley & Company, LLP
1030 15th Street, NW
Washington, DC 20005**

September 2011




UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

Information Technology Audit Division

September 30, 2011

Memorandum

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

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

SUBJECT: Final Audit Report
Education Department Utility for Communications, Applications, and Technology
Environment (EDUCATE) Information Security Audit
Control Number ED-OIG/A11L0001

Attached is the **final audit report** that determined whether the Department has developed and implemented adequate information system security controls to properly secure and safeguard EDUCATE and the Department's data in accordance with the Federal Information Security Management Act and the Office of Management and Budget and National Institute of Standards and Technology regulations and standards. We contracted with the independent certified public accounting firm of Williams, Adley & Company-DC, LLC (Williams Adley) to conduct this audit. The audit assessed the information and information system security controls in place during the period October 1, 2010, through April 30, 2011.

The contract required that the audit be performed in accordance with generally accepted government auditing standards (GAGAS). In connection with the contract, the Office of Inspector General (OIG) reviewed, provided feedback, and ultimately approved the audit plan, monitored the performance of the audit, reviewed contractor audit documentation, attended critical meetings with Department officials and reviewed the contractor's audit controls. The review was designed to help ensure that:

- the audit complied with GAGAS and other OIG policies and procedures (to include the completion of OIG Performance Audit Quality Assurance Checklists that reflect GAGAS requirements, OIG's Field Work Standards for Performance Audits, and mandatory requirements contained in the OIG Policies and Procedures Manuals);
- contract requirements regarding objectives, scope and methodology were being met;
- monthly status meetings to discuss whether milestones were being met; and
- draft and final audit report reviews conducted within Information Technology Audits and Computer Crime Investigations provided the assurance that the contractor's work can be relied on.

An electronic copy has been provided to your Audit Liaison Officer. We received and evaluated the Office of the Chief Information Officer (OCIO) management comments and the corrective action plan for each of the recommendations contained in the draft report. Appendix B of the report incorporates OCIO's management responses to each of the findings. We have modified recommendations where appropriate to address management comments.

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). Department 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 6 months from the date of issuance.

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

Williams Adley is responsible for the enclosed auditor's report and the conclusions expressed therein. The OIG's review disclosed no instances where Williams Adley did not comply, in all material aspects, with GAGAS.

Should you or your office have any questions, please contact Joseph Maranto at 202-245-7044, or joseph.maranto@ed.gov.

Enclosure

cc: Michele Iversen, Director, Office of the Chief Information Officer
Dana Stanard, Audit Liaison, Office of the Chief Information Officer
Bucky Methfessel, Senior Counsel for Information & Technology, Office of General Counsel
L'Wanda Rosemond, AARTS Administrator, Office of Inspector General



September 28, 2011

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

Ms. Sherri Demmel
Deputy Assistant Inspector General for Information
Technology Audits and Computer Crimes Investigations

U.S. Department of Education
Office of Inspector General
Washington, D.C.

**RE: Education Department Utility for Communications, Applications, and Technology
Environment Information Security Audit**

Williams, Adley & Company, LLP (referred to as “we” in this letter), is pleased to provide the Office of Inspector General (OIG) the results of our review and independent assessment of the U.S. Department of Education (Department) information and information systems security program controls over the Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE). The purpose of the audit was to determine whether the Department has developed and implemented adequate information system security controls to properly secure and safeguard EDUCATE and the Department’s data in accordance with the Federal Information Security Management Act and the Office of Management and Budget and National Institute of Standards and Technology regulations and standards. We assessed the information and information system security controls in place during the period October 1, 2010 through April 30, 2011.

This review, performed under Contract No. ED-08-DO-0046, was designed to meet the objectives identified in Appendix A, “Objectives, Scope, and Methodology,” of the report. We conducted the audit in accordance with Government Auditing Standards and communicated the results of our review and the related findings and recommendations to the Department’s OIG. We also communicated the conditions and causes of the conditions to the Office of the Chief Information Officer.

We appreciate the cooperation provided by Department personnel during the review and the assistance provided by the OIG.

Williams, Adley & Company, LLP
Washington, DC

Table of Contents

ACRONYMS/ABBREVIATIONS/ SHORT FORMS USED IN THIS REPORT	III
I. EXECUTIVE SUMMARY	1
II. BACKGROUND	4
III. RESULTS OF REVIEW.....	6
1. Security Configuration Management Process Needed Improvement	6
2. Network Security Controls over Hardware Devices and Software Needed Improvement	9
3. Security Patch Management Process Needed Improvement	10
4. Remote Access Software Was Not Compliant with OMB and NIST Standards	12
5. Perot Systems Network Operating System Controls for Identifying and Resolving Vulnerabilities Needed Improvement	14
6. The Department's Incident Response Program Needed Improvement to Ensure Timely and Appropriate Detection, Reporting, and Resolution of Computer Security Incidents to Internal and External Parties.....	15
7. Account and Identity Management Processes Required Significant Improvement	17
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	19
9. Federal Desktop Core Configuration Security Configuration Management Process Needed Improvement	22
10. The Department Needed to Update the Security Assessment and Authorization Documents.....	23
11. Contingency Planning Program Needed Improvement.....	25
12. The Department Needed to Establish an Organization-Wide Risk Management Strategy.....	27
13. Documentation of Security Awareness Training Needed Improvement.....	29
14. Plan of Action and Milestones Process Was Not Adequately Managed.....	30
APPENDIX A: OBJECTIVES, SCOPE, AND METHODOLOGY	33
APPENDIX B: OFFICE OF CHIEF INFORMATION OFFICER COMMENTS	37

Acronyms/Abbreviations/ Short Forms Used in this Report

AT	Awareness Training
BCP	Business Contingency Plan
BIA	Business Impact Analysis
CAMS	Case Activity Management System
CAT	Category
CCE	Common Configuration Enumeration
CCP	Configuration Control Process
CM	Configuration Management
COCO	Contractor Owned and Contractor Operated
COOP	Continuity of Operation Plan
CSAM	Cyber Security and Management
CVE	Common Vulnerabilities and Exposures
Department	U.S. Department of Education
DHS	Department of Homeland Security
DLL	Dynamic Link Library
DoS	Denial of Service
DRP	Disaster Recovery Plan
EARB	Enterprise Architecture Review Board
EDCIRC	Education Incident Response Coordinator
EDCIS	EDUCATE Data Center Information System
EDNIS	Education Network Infrastructure System
EDMASS	EDUCATE Mass Storage System
EDSOC	EDUCATE Security Operations Center
EDUCATE	Education Department Utility for Communications, Applications, and Technology Environment
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
FIPS PUB	Federal Information Processing Standards Publications
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
IA	Information Assurance
IAS	Information Assurance Services
IP	Internet Protocol
IPAR	Investigative Program Advisory Report
ISA	Interconnection Security Agreement
ISSO	Information System Security Officer
IT	Information Technology
LM	Local Area Network Manager
MOU	Memorandum of Understanding
MSSP	Managed Security Service Provider
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General

OMB	Office of Management and Budget
OVMS	Operational Vulnerability Management System
PII	Personally Identifiable Information
PIA	Privacy Impact Assessment
POA&M	Plan of Action & Milestones
Rlogin	Remote login
RSA	Rivest, Shamir and Adleman
SCAP	Security Content Automation Protocol
SHA	Secure Hash Algorithm
SLA	Service Level Agreement
SMB	Server Message Block
SOP	Standard Operating Procedures
SQL	Structured Query Language
SP	Special Publications
SSH-1	Secure Shell Version 1
SSO	System Security Officer
SSP	Systems Security Plan
STIGs	Department of Defense Security Technical Implementation Guides
TACACS+	Terminal Access Controller Access Control System Plus
TFMS	Treasury Financial Management System
TSP	Telecommunication Service Priority
US-CERT	U.S. Computer Emergency Response Team

I. Executive Summary

The purpose of the audit was to determine whether the U.S. Department of Education (Department) has developed and implemented adequate information systems security controls to properly secure and safeguard the Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) and the Department's data in accordance with the E-Government Act (Public Law 107-347), including Title III, the Federal Information Security Management Act of 2002 (FISMA) and the Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) regulations and standards. We have concluded that the Department's information systems security program controls over EDUCATE need improvement to address the 14 operational, managerial, and technical security control weaknesses identified in this report. The following control weaknesses need improvement:

1. Security Configuration Management
2. Network Security Controls Over Hardware Devices
3. Security Patch Management
4. Remote Access Software
5. Network Vulnerabilities
6. Incident Response Program
7. Account and Identity Management Processes
8. Education Network Infrastructure System (EDNIS) System Security Plan and Update Procedures
9. Federal Desktop Core Configuration (FDCC) Configuration Management Process
10. Security Assessment and Authorization Documents
11. Contingency Planning Program
12. Organization-Wide Risk Management Strategy
13. Documentation of Security Awareness Training
14. Plan of Action and Milestones

Based on our review, the causes of the security control weaknesses generally fall into the following areas:

- Office of the Chief Information Officer (OCIO) monitoring and oversight controls are not sufficiently designed or implemented to ensure contractor compliance with Federal requirements.
- OCIO did not develop its policies, procedures, and processes to obtain assurance of the contractor's performance under the current contractual arrangement.
- The Department's internal control procedures are not sufficient to ensure that system owners and other responsible parties perform their assigned duties in a timely manner.

The EDUCATE contract was entered into by the Department with a third party information technology (IT) service provider, Perot Systems.¹ It established a Contractor Owned and Contractor Operated (COCO) service model under which the contractor operates the Department's IT infrastructure (hardware, communication devices, and operating systems) on a 24/7/365 basis. Under the COCO contract, OCIO retains the responsibility to monitor and oversee the contractor's performance, while the contractor is responsible for operating, maintaining, and supporting the Department's IT infrastructure. Additionally, OCIO is responsible for ensuring that the contractor's information system security controls meet or exceed the Department's requirements and Federal laws, regulations, and standards.

Our audit was limited to a review and test of the information security controls covering the EDUCATE subsystems: Education Data Center Information System (EDCIS), EDNIS, EDUCATE Mass Storage System (EDMASS), EDUCATE Security Operations Center (EDSOC), Department of Education's Central Automated Processing System (EDCAPS), and Case Activity Management System (CAMS); and the wide-area and local-area network hardware consisting of network servers, routers, switches, and external firewalls. Our review also covered tests of the network gateways to the Internet. We also conducted internal and external network vulnerability analyses.

This report contains specific recommendations that require OCIO to strengthen existing controls and to develop new monitoring capabilities designed to ensure OCIO and contractor's compliance with Federal information system security laws, regulations, and standards. Additionally, the recommendations are designed to ensure that the Department's sensitive and financial data and systems processed and maintained by the contractor are properly secured and safeguarded from unauthorized system access and fraudulent activities. Further, the recommendations are designed to ensure that the network and systems information security controls are properly implemented and maintained to adequately safeguard the Department's data from unauthorized modification and release and to provide an adequate level of auditability.

As discussed in greater detail in this report, the EDUCATE password security control weaknesses enabled the auditors to gain access to one EDUCATE server administrator's account. Additionally, our tests disclosed that the internal security control weaknesses could enable Department users and contractor personnel to exploit various network vulnerabilities. These weaknesses could enable the implementation and installation of unauthorized software and hardware devices onto the network to perform unauthorized activities such as modifying data without detection. The user account identity control weaknesses could also provide internal users with opportunities to masquerade as other users to perform unauthorized activities such as fraud without disclosure of the actual person performing the fraudulent activities.

We commend OCIO for taking positive actions to implement new and enhanced controls to address information systems security control weaknesses previously identified and reported to OCIO by the Office of Inspector General (OIG) in the OIG reports entitled "Department's Processes for Validating the EDUCATE Contractor's Performance" (ED-OIG/A19K0007), dated May 2011, and the "2010 Annual FISMA Report." We also commend OCIO for taking action to

¹ Perot Systems was acquired by Dell in September 2009.

supplement the Service Level Agreement (SLA) during the audit to improve information security controls to address control weaknesses previously identified. On April 1, 2011, OCIO and Perot Systems entered into an agreement to add additional performance measures to the SLA. OCIO updated the SLA to include specific language for incident response reporting and security infrastructure software, which addressed security weaknesses identified during the audit.

The audit assessed and tested the information security controls in place at Perot Systems' Data Center located in Plano, Texas, and the Department's controls at the Washington, DC, headquarters. We conducted the audit during the period October 1, 2010 through April 30, 2011.

In its response to the draft audit report, OCIO stated that the report provided insight into the effectiveness of information systems security controls in place to secure the EDUCATE environment, and accurately identifies several areas that need improvement. OCIO concurred with 37 of the 42 recommendations and partially concurred with Recommendations 13.1 and 13.2. OCIO did not concur with Recommendations 8.4, 11.2, and 12.4.

We evaluated OCIO's comments related to our recommendations and the corrective actions OCIO has taken since April 2011, or has proposed to take to address the control weaknesses. However, we have not verified whether the corrective actions OCIO has taken corrected the cited deficiencies. Where necessary, we modified the recommendations in response to OCIO's comments.

During our fieldwork, we engaged in many discussions with applicable Department officials and staff, including senior OCIO management and Dell officials, to clarify the weaknesses noted and to provide clarification on recommendations. We also provided documents and other material to OCIO personnel for their review.

II. Background

The U.S. Department of Education (Department) entered into a contract with Perot Systems² to manage and provide all IT infrastructure services to the Department under the Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) system. The contract established a Contractor Owned and Contractor Operated (COCO) information technology (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, performance-based, indefinite delivery/indefinite quantity contract with fixed unit prices. Under the COCO contract, Perot 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.

Our audit was limited to a review and test of the information security controls covering the EDUCATE subsystems: 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) and the wide-area and local-area network hardware consisting of network servers, routers, switches, and external firewalls. Our review also covered tests of the network gateways to the internet. We also conducted internal and external network vulnerability analyses.

Under the COCO contract, the contractor is responsible for operating, managing, and maintaining information and an information system security program compliant with Federal requirements. Further, the contractor is responsible for the day-to-day security and operational activities including but not limited to:

- Installing vendor provided operating system updates and security patches
- Configuring hardware devices based on configuration management rules
- Performing security administration activities for establishing and removing users' accounts to the network and applications
- Establishing, modifying, and removing users' privileges within the network and applications based on system owners' and information security officers' direction
- Performing continuous network security monitoring
- Reporting incident response
- Performing backup of the network, databases, and software
- Developing and implementing procedures and processes for restoring the IT infrastructure in the event of a disaster or other event that causes a disruption to the network service

² Perot Systems was acquired by Dell in September 2009.

We evaluated the EDUCATE information systems security controls against the Federal laws, regulations, and standards as specified in FISMA; OMB Circulars A-130 “Management of Federal Information Resources,” Appendix III, “Security of Federal Automated Information Resources,” A-127 “Financial Management Systems,” and A-123 “Management Accountability and Control,” Section III, Assessing and Improving Management Controls, and Section IV Correcting Management Control Deficiencies; the NIST Federal Information Processing Standards (FIPS) Publication Standards 199 – “Standards for Security Categorization of Federal Information and Information Systems,” dated February 2004, and “200 Minimum Security Requirements for Federal Information and Information Systems,” dated March 2006; various NIST Special Publication (SP) Series 800 such as 800-53 Revision 3 “Recommended Security Controls for Federal Information Systems and Organizations,” dated August 2009, and 800-53A “Guide for Assessing the Security Controls in Federal Information Systems,” and “Building Effective Security Assessment Plans,” dated July 2008. Additional NIST SPs used in the evaluation included SP 800-63, Revision 1.0.2, “Electronic Authentication Guide,” dated April 2006; SP 800-37 “Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems,” dated February 2010; SP 800-30 “Risk Management Guide for Information Technology Systems,” dated July 2002; SP 800-18 Revision 1 “Guide for Developing Security Plans for Information Systems,” dated February 2006; NIST SP 800-128 “Guide for Security Configuration Management of Information Systems,” (Draft) dated March 2010; and SP 800-61, Revision 1, “Computer Security Incident Handling Guide,” dated March 2008.

III. Results of Review

Based on our audit, we conclude that the Department's information and information systems security program controls over EDUCATE need improvement to address the 14 operational, managerial, and technical security control weaknesses identified in this report. From the information provided, the causes of the security control weaknesses generally fall into the following areas:

- OCIO monitoring and oversight controls are not sufficiently designed or implemented to ensure contractor compliance with Federal requirements.
- OCIO did not develop its policies, procedures, and processes to obtain assurance of the contractor's performance under the current contractual arrangement.
- The Department's internal control procedures are not sufficient to ensure system owners and other responsible parties perform their assigned duties in a timely manner.

This report contains specific recommendations that require OCIO to enhance existing controls and to develop new monitoring capabilities designed to ensure OCIO and Perot Systems' compliance with Federal information and information system security laws, regulations, and standards. Additionally, the recommendations are designed to ensure that the Department's sensitive and financial information processed and maintained by the contractor are properly secured and safeguarded from unauthorized access and activities. Further, the recommendations are designed to ensure that the network and information systems security controls are properly implemented and maintained to adequately safeguard the Department's information from unauthorized modification and release and to provide an adequate level of auditability.

The audit assessed and tested the information security controls in place at the contractor's data center located in Plano, Texas, and at the Department's OCIO and other Program Offices during the period October 1, 2010 through April 30, 2011.

To assist OCIO in understanding the audit results, we have presented the audit results in order of highest risk to lowest risk.

1. Security Configuration Management Process Needed Improvement

Although Perot Systems performs monthly scans of the network, vulnerabilities in the security configuration continued to exist. We used the Department of Defense Security Technical Implementation Guides (STIGs) to conduct our review and tests of the network devices. Based on our reviews and tests of the software configuration for 25 EDUCATE servers, switches, routers, and databases, we found the following significant high-risk vulnerabilities with the configurations:

- 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.

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

Detailed information on the vulnerabilities was given to OCIO for remediation.

FISMA requires each agency to develop minimally acceptable system configuration requirements and ensure compliance with them. Standard security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. In the annual FISMA report to OMB, agencies are required to document the frequency with which they implemented system configuration requirements and must document any deviation from common security configurations.

We also found that OCIO had not established monitoring and reporting procedures to track and approve changes to the hardware operating systems designed to resolve network security configuration vulnerabilities. Additionally, OCIO had not established reporting procedures to require Perot Systems to report on the status of installing vendor security patches and recommended operating system configuration changes designed to address known vulnerabilities.

NIST SP 800-53, Revision 3, requires agencies to establish a continuous monitoring strategy and implement a continuous monitoring program and a configuration management process. It also requires an agency to assess the security impact of configuration changes to the information system and environment and to report on the security state of the information system. This guidance also requires agencies to develop controls to ensure implementation of approved configuration settings; to identify, document, and approve exceptions from the mandatory configuration settings; and to monitor changes to the configuration settings in accordance with organizational policies and procedures.

Additionally, Sections 3.4.2, Tools for Monitoring Secure Configurations and 3.5, Using Security Content Automation Protocol (SCAP) of NIST SP 800-128, Guide for Security Configuration Management of Information Systems (Draft) dated March 2010, provides additional guidance for assessing networks hardware devices for managing configurations. NIST SP 800-128 specifically recommends that an agency should consider a tool that can automatically assess configuration settings of IS components within the information environment. An automated tool should be able to scan different information system components (e.g., Web server, database server, network devices, etc.) running different operating systems, identify the current configuration settings, and indicate where they are noncompliant with policy.

Perot Systems did not document the reasons for not remediating vulnerabilities in accordance with OMB Circular A-130, Appendix III, and NIST SP 800-53A, which would permit OCIO to assess the potential effect of the vulnerability versus the costs associated with implementing the

suggested corrective action. OMB Circular A-130 Appendix III and NIST SP 800-53A, specifically require agencies to assess and evaluate the cost of implementing controls versus the benefits to be derived in implementing security controls as part of the overall risk assessment process.

Also, the EDUCATE SLA procedures and processes do not require the use of a specific scanning software such as STIG automated tools that would allow Perot to identify security vulnerabilities with configuration settings within the operating systems for clients and servers, databases, and network infrastructure devices (firewalls, routers, and switches) supporting EDUCATE.

Poor configuration management practices for the operating systems increases the potential for unauthorized activities to occur without being detected thus leading to potential theft, destruction, and misuse of agency data both from internal and external threats.

RECOMMENDATIONS:

We recommend OCIO:

- 1.1 Revise the SLA to require Perot Systems to take appropriate timely corrective action to resolve network security configuration vulnerabilities or to justify not implementing suggested corrective action to permit OCIO to assess the potential effect of the vulnerability versus the costs associated with implementing the suggested corrective action.
- 1.2 Revise the SLA to require Perot Systems to use various scanning software such as STIG and Security Content Automation Protocol (SCAP) tools, as well as the STIG checklist. The security scanning software should be compliant with the NIST SP 800-128 (Draft) to identify security vulnerabilities within the operating systems for clients and servers, databases, and network infrastructure devices (firewalls, routers, and switches) supporting EDUCATE.

Management Response

OCIO concurred with Recommendations 1.1 and 1.2. However, in its response, OCIO provided suggested wording change for Recommendation 1.2.

OIG Response

We did not agree with OCIO's suggestion to develop and implement policies and procedures instead of revising the SLA. Unless the SLA is modified, Perot Systems will not be legally required to comply with the policies and procedures. However, we did revise the recommendation to include SCAP automated tools, as well as the STIG checklist. Including STIG compliant tools will ensure that anything that is not covered by SCAP will be covered by STIG. Also, including the STIG checklist will further ensure that anything not identified by STIG and SCAP automated tools will be addressed.

2. Network Security Controls over Hardware Devices and Software Needed Improvement

Our review of EDUCATE hardware and software accountability security controls found the following deficiencies:

- Perot Systems reported 1,675 work stations 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 UNIX³ servers sampled from a population of 363 servers.
- In their monthly scan reporting process, neither 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.

NIST SP 800-53, Revision 3, Appendix F Family Configuration Management (CM)-8, Information System Component Inventory, dated August 2009, requires an agency to develop, document, and maintain an inventory of information system components that does the following:

- accurately reflects the current information system;
- is consistent with the authorization boundary of the information system;
- is at the level of granularity deemed necessary for tracking and reporting;
- includes information deemed necessary by the Department to achieve effective property accountability; and
- is available for review and audit by designated organizational officials.

OCIO in conjunction with Perot Systems had not developed policies or procedures to fully account for hardware and software installed or permitted to be used on the EDUCATE network. OCIO did not require Perot Systems to resolve the reporting variances or to provide an explanation for the variances, such as undetermined operating systems and unknown host names.

Without accurate accountability of the hardware and software permitted to be installed on the network or to be connected or installed on the network, OCIO increases the risk that unauthorized hardware may be connected or installed on the network that may permit unauthorized activities to occur and go undetected for an extensive period of time.

³ Uniplexed Information and Computing System

RECOMMENDATIONS:

We recommend OCIO in conjunction with Perot Systems:

- 2.1 Develop and implement policies and procedures to fully account for software or hardware installed or permitted through exception to be used on the EDUCATE network.
- 2.2 Revise the SLA requirements to require Perot Systems to implement procedures to carry out its responsibility for ensuring that only authorized devices are permitted to be installed on the network and to verify the number of devices permitted on the EDUCATE network or to obtain a reliable accountability of hardware.
- 2.3 Require Perot Systems to resolve the monthly reporting variances, such as undetermined operating systems and unknown host names within 5 working days.
- 2.4 Require Perot Systems to terminate the network connections and authorizations for hardware labeled as “undetermined.”

Management Response

OCIO concurred with Recommendations 2.1 through 2.4. However, OCIO requested a modification to Recommendation 2.1 to delete the words “or permitted to be used.” OCIO stated in its response that the Department’s Enterprise Architecture Review Board (EARB) maintains an End User Catalog of software and hardware that are permitted to be installed on the EDUCATE network. Additionally, OCIO outlined efforts to detect rogue devices installed on the network but did not address efforts to detect rogue software that may be running on the network. OCIO stated that Recommendations 2.3 and 2.4 have been completed, but we did not verify that the corrective action corrected the deficiencies cited.

OIG Response

We reviewed management’s response and did not agree to delete the words “or permitted to be used” from Recommendation 2.1. However, we modified the recommendation to include the words “through exception” to acknowledge software and hardware that are permitted to be used on the network by individual exception. Individual exceptions address specific job/function requirements that may exist only in one area of the Department (e.g., OCIO), and those exceptions are not approved by the EARB. In its response, OCIO stated that Dell Systems has a process for identifying rogue devices. Additionally, OCIO stated it has begun engineering analysis to pilot network access control software. Network access control software compares authorized hardware to what is installed; however, it does not identify rogue software or software that is permitted to run on the network through exception.

3. Security Patch Management Process Needed Improvement

We conducted tests of the security patch management installation processes and procedures to determine whether the security patch management process ensured that critical security patches

were installed in a timely manner. Because the Department had not defined timeframes for installing critical security patches onto servers, the auditors elected to measure performance using the Dell End User Computing Workstation Patch and Configuration Management Process. Section 7 of Dell's process states that for an "Urgent" patch, Dell will initiate the patch within 3 days and complete the deployment within 30 days; and for a "High" patch, Dell will initiate the patch within 5 days and complete the deployment within 30 days.

Our tests disclosed that OCIO had not defined timeframes for installing security patches on network devices in the SLA with Perot Systems. Our review of the Perot Systems' patch management processes disclosed that Perot Systems 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 our sample of 25 devices consisting of 19 servers and 6 switches, we found that Perot had not installed critical security patches for 16 servers; however, we found that Perot 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. OCIO was not aware that Perot had not installed security patches on all network devices within the timeframe required by Dell's process (30 days).

NIST SP 800-53, Revision 3, CM-8, Information System Component Inventory, dated August 2009, requires an agency (including any contractor to the agency) to promptly install security-relevant software updates (e.g., patches, service packs, and hot fixes).

OCIO had not established the procedures within the original SLA to obtain assurance that Perot had implemented security patches in a timely manner. During the audit, OCIO updated the SLA to include a 30-day timeframe for completing installation of security patches. However, there was no mention of timeframes for initiating security patches in the updated SLA. Additionally, the original SLA did not require Perot to provide a detailed performance report that would disclose the following:

- number of security patches released by vendors within the past reporting period;
- criticality of the security patch and the number of network devices affected by the security patch;
- number of devices patched; and
- number of devices remaining to be patched.

Failure to implement security patches in a timely manner increases the potential for unauthorized access and exploitation of security vulnerabilities that can result in unauthorized release of sensitive data, modification of data, and theft of data.

RECOMMENDATIONS:

We recommend OCIO:

- 3.1 Amend the SLA to establish detailed performance reporting factors that would disclose the number of security patches released by vendors within the past reporting period, the criticality of the security patch, the number of network devices affected by the security

patch, the number of devices patched, and the number of devices remaining to be patched.

3.2 Amend the SLA to include language that would require contractors to initiate the installation of vendor security patches within a 3-day period from the vendor release date or provide OCIO with a justification for not installing the security patch.

3.3 Require Perot Systems to report monthly on the security patches received by the vendor but not installed during the period and include a schedule for installing the patch.

Management Response

OCIO concurred with Recommendations 3.1 through 3.3.

4. Remote Access Software Was Not Compliant with OMB and NIST Standards

The EDUCATE network software that controls remote access settings was not compliant with OMB and NIST requirements. We noted the following deficiencies based upon our testing:

1. 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.
2. 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.

NIST SP 800-57 Part 3 recommends using Rivest, Shamir and Adleman (RSA) 2048 with an algorithm of secure hash algorithm (SHA) 256 for a Certificate Authority. For a certificate generated after December 31, 2010, the public key is also recommended to be RSA 2048 with an algorithm of SHA 256. Further, OMB Memorandum 07-16 requires agencies to use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes of inactivity and 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.

On September 16, 2010, OIG issued an Investigative Program Advisory Report (IPAR), Weaknesses in the Process for Handling Compromised Privileged Accounts (09-220005) Control Number L21K0002 to the Deputy Secretary and Federal Student Aid (FSA). OIG determined FSA did not identify all individuals whose data were potentially compromised; the Department and FSA failed to conduct adequate log reviews of compromised privileged accounts to identify unauthorized activity; FSA kept inadequate records of its remediation efforts for compromised privileged accounts; and the Department and FSA did not require two-factor authentication for

remote access to Department and FSA systems. OIG also made recommendations that the Department (1) identify all potentially compromised personally identifiable information (PII) by analyzing all account activity during the period that the privileged account was compromised; (2) revise current methodology used to identify suspicious activity that indicates unauthorized access into privileged accounts; (3) track compromised accounts and PII and the date of compromise, account deactivations, owner/borrower notifications, and the date and results of the account log review; and (4) implement two-factor authentication on any system where a user can log into a privileged account from the Internet, with an emphasis placed on financial systems and systems containing large volumes of PII.

As far back as July 2007, OIG reported weaknesses in the Department's and FSA's response to compromised privileged accounts. Although the Department and FSA have started implementing two-factor authentication for some employees, to date not all Department employees and external users who log in remotely or through a Web site to gain access to Department systems are required to use two-factor authentication. This includes privileged external users at guaranty agencies, lenders, servicers and post secondary institutions who pose a great risk to Department systems. The computer systems owned by external partners are not secured by the Department and are generally not required to comply with Federal and Department standards.

Based on our review of documentation and discussions with OCIO officials, we determined that the EDUCATE network software that controls remote access settings does not comply with OMB and NIST requirements, because the Department did not establish controls within the SLA to require two-factor authentication or to ensure Perot complied with NIST encryption software requirements as changes are implemented by NIST and OMB.

Without effective encryption process communication between a remote user's computer and Department servers, those servers are at increased risk of unauthorized access if the connection is established with a noncompliant digital certificate and bit encryption. Additionally, the lack of a multifactor authentication to the EDUCATE network increases the risk of an unauthorized user accessing the network remotely and misusing, altering or destroying sensitive Department data.

RECOMMENDATIONS:

We recommend OCIO:

- 4.1 Require Perot Systems to change the digital certificate and bit encryption for remote servers to the recommended settings that are specified in NIST 800-57 Part 3.
- 4.2 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 (09-220005), Control Number L21K0002.

Management Response

OCIO concurred with Recommendations 4.1 and 4.2.

5. Perot Systems Network Operating System Controls for Identifying and Resolving Vulnerabilities Needed Improvement

We performed vulnerability scans of the EDUCATE network. Based on our external vulnerability scans of the EDUCATE network, we identified a Department Web site that is vulnerable to Structured Query Language (SQL) injection⁴ attacks that allow an attacker to read, update, or delete database records from the Internet.

We also performed internal network vulnerability scans and identified the following high-risk vulnerabilities:

- Five Terminal Access Controller Access Control System Plus (TACACS+) 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 (Rlogin), which allows network administrators to login and send their credentials in clear-text, making them susceptible to packet analysis.
- Nine network devices use Secure Shell Version 1 (SSH-1), which allows data to be exchanged using a secure channel. However, multiple vulnerabilities exist making 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.

Detailed information on the vulnerabilities was given to OCIO for remediation.

NIST SP 800-53, Revision 3, Appendix F, Remote Access 5, Vulnerability Scanning requires agencies to conduct periodic scans of the network to identify vulnerabilities and to establish processes to remediate vulnerabilities using a risk-based approach.

Perot Systems has not updated the operating system with security patches for the various devices noted above as recommended by the software vendor and as required by the NIST SP 800-53, Revision 3.

Failure to perform periodic scans and other tests of the network operating systems increases the risk that known operating system vulnerabilities for various devices connected to the network

⁴ SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application.

may be exploited by unauthorized individuals leading to the theft, destruction, or misuse of sensitive data and Departmental assets.

RECOMMENDATIONS:

We recommend OCIO:

5.1 Direct Perot Systems to take immediate action to address the vulnerabilities identified and report to OCIO on the schedule for implementing the remedial action.

5.2 Direct Perot Systems to enhance its current operating procedures to perform network scans every two weeks or more frequently as necessary.

Management Response

OCIO concurred with Recommendations 5.1 and 5.2.

6. The Department's Incident Response Program Needed Improvement to Ensure Timely and Appropriate Detection, Reporting, and Resolution of Computer Security Incidents to Internal and External Parties

The Department must be capable of properly responding to incidents in a timely manner and to rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. FISMA requires Federal agencies to create and operate a formal incident response capability. Additionally, NIST SP 800-61, Revision 1, "Computer Security Incident Handling Guide," dated March 2008, requires Federal agencies to report incidents to the United States Computer Emergency Readiness Team (US-CERT) office within the Department of Homeland Security (DHS). The requirement to report to US-CERT is essential to safeguarding Federal IT assets from the migration of IT threats, such as viruses from one agency to another, and to informing Federal managers of identified security breaches so that Federal managers can institute appropriate preventive measures.

On June 14, 2011, OIG issued an IPAR, Incident Response and Reporting Procedures (10-1102832) Control Number L21L0001 to OCIO. OIG determined that 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 Procedures*". The report cited specific instances, dating back to March 2009, where Perot System did not follow OCIO-14 and NIST SP 800-61 protocols to collect 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. Specifically, the current practice by Perot Systems once an incident is discovered is to remove the infected system from the network and attempt to clean the system by running a virus scan before there is any attempt to collect potential evidence. The report concluded that the deficiencies have left the Department's systems and data vulnerable. OIG also made recommendations to the Chief Information Officer to 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: (1) providing incident response personnel with the appropriate training and tools to collect and preserve evidence in a quick and forensically sound manner; (2) analyzing information to determine the root cause of an incident and to determine the extent of damage; and (3) 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.

To determine whether OCIO was compliant with NIST incident reporting requirements, we selected 15 incident tickets for testing. Our tests disclosed the following:

- Two of 15 Operational Vulnerability Management System (OVMS) security incidents were not reported to 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 categorized as Category (CAT) 3.
- Four of 15 OVMS security incidents were not resolved in a timely manner to prevent further damage. Specifically, 3 of 4 security incidents, which were CAT 3 EINSTEIN alerts identified by US-CERT, were reported 14, 16, and 27 days after the incident, and one CAT 1 incident was reported 14 days late.

NIST SP 800-61, Revision 1, requires agencies to establish incident response procedures in compliance with US-CERT reporting requirements. OCIO-14, "Handbook for Information Security Incident Response and Reporting Procedures" dated March 2, 2011 also defines the reporting requirements, which are included in the EDUCATE SLA. NIST has defined CAT 1, 2, and 3 incidents and requires agencies to report within the specific timeframe.

Category	Incident Type	Description	Reporting Timeframe
CAT 1	Unauthorized Access	A person gains logical or physical access without permission to a Federal agency network, system, application, data, or other technical resource.	Within one (1) hour of discovery/detection.
CAT 2	Denial of Service (DoS)	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	Malicious Code	A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host. Agencies are NOT required to report malicious logic that has been <i>successfully quarantined</i> by antivirus software.	Daily Note: Within one (1) hour of discovery / detection if widespread across agency.

Based on our review of documents and discussions with OCIO officials, we determined that the control weaknesses cited were caused by ineffectively designed internal controls. Specifically,

OCIO did not develop procedures for reporting and resolving security incidents within the required timeframes in OVMS, or in OCIO-14. Additionally, Education Incident Response Coordinator (EDCIRC) procedures did not require following up on Perot Systems' compliance with the US-CERT Federal reporting timeframe for CAT 3 incidents, which should be reported daily. OCIO monitoring procedures were not effectively designed to monitor Perot's performance specifically with resolving security incidents in the required manner and timeframe as specified in the EDUCATE SLA.

Not properly responding to computer security incidents violates the containment procedures set forth in OCIO-14, hampers the investigative processes that is part of the detection/identification phase, and can destroy the potential for determining the root cause of the incident. Because malicious code (as defined by US-CERT in the above table) works surreptitiously and can propagate to other systems rapidly, early containment of a malicious code incident is needed to stop it from spreading and causing further damage. Additionally, if a security incident is identified on the network, it could spread organization-wide if not resolved in a timely manner. Further, not developing an internal timeframe for resolving incidents may delay or prevent eradicating an incident within the expected timeframe and holding responsible individuals fully accountable.

RECOMMENDATIONS:

We recommend OCIO:

- 6.1 Require Perot Systems to comply with the EDUCATE SLA for resolving incidents within the SLA specified timeframe.
- 6.2 Continue its efforts to work with Perot Systems to address the issues cited in the IPAR, Incident Response and Reporting Procedures (10-1102832) Control Number L21L0001.

Management Response

OCIO concurred with Recommendations 6.1 and 6.2.

7. Account and Identity Management Processes Required Significant Improvement

User account and identity management is an essential security operational function that restricts access to mission critical systems to only authorized users for only authorized purposes. Our tests were designed to determine whether OCIO had designed and implemented effective processes and procedures to ensure that only authorized individuals were granted access to EDUCATE and that any unnecessary accounts are either removed or deactivated. From our tests of the Active Directory user account management functions, we found the following deficiencies within the Account and Identity Management process. From a population of approximately 6,997 active accounts in Active Directory, we found the following:

- 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 the EDNIS and EDCIS System Security Plan (SSP), 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.⁵ 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.

From a population of 37 voluntarily separated employees, we found that management had not disabled the accounts of 8 of these employees within the required timeframe. According to OCIO-01 “Handbook for Information Assurance Security Policy,” dated March 31, 2006, supervisors must notify system administrators within 2 business days of the departure of separated employees and contractors, and system access shall be terminated as soon as possible, but no later than 2 business days of notification. Additionally, the SLA states that once notified by the Department, the user account will be disabled within one hour.

EDCIS and EDNIS SSPs, dated June 17, 2010, and June 19, 2009, respectively, states:

- Accounts that have not logged on to the EDCIS and EDNIS for more than 90 days are deactivated.
- Password expiration should be enabled for all users.
- All users are required to periodically change their password.

OCIO-01 states that users’ system access for terminated employees will be terminated within 2 days of departure.

OCIO had not developed policies to provide guidance to ensure that Perot was compliant with NIST standards and OCIO policies for account and identity management. OCIO did not require Perot to provide a report listing changes to active user accounts or to ensure that:

- Active user accounts within Active Directory have been used within the last 90 days.
- Accounts require a password and that all account passwords must be changed every 60 or 90 days.
- Unnecessary accounts have been removed.
- Accounts associated with employees’ terminated or separated from the Department have been removed or de-activated.

Inadequate account and identity management processes increase the risk that temporary and active accounts may be accessed by Department and contractor personnel to perform

⁵ 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.

unauthorized activities, such as modifying or improperly releasing sensitive Department information. Additionally, accounts set with passwords that do not expire increase the potential for an account password to be obtained resulting in the use of the account by unauthorized users.

RECOMMENDATIONS:

We recommend OCIO:

- 7.1 Ensure that Active Directory is annually reviewed for access privileges of users.
- 7.2 Configure the Active Directory account management automated tools to flag accounts that have not been used and ensure that all accounts are configured with passwords that have an expiration date.
- 7.3 Revise the SLA to include a performance incentive or penalty clause to enforce OCIO account management policies such as disabling inactive accounts and terminating accounts of separated employees.

Management Response

OCIO concurred with Recommendations 7.1 through 7.3.

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

Our review of 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 Interconnection Security Agreement (ISA) or a Memorandum of Understanding (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.

We also determined that for the four external connections, neither the EINSTEIN⁶ nor the Managed Security Service Provider (MSSP) intrusion detection systems had an MOU.

⁶ EINSTEIN is the US-CERT automated process for collecting, correlating, analyzing, and sharing computer security information across the federal government to improve our nation's situational awareness.

Additionally, the Treasury Financial Management System (TFMS) and Department of Justice Cyber Security Assessment and Management (CSAM) MOU and ISA agreements had not been reviewed within the past 2 years. Further, 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.

OCIO Handbook-15, "Handbook for Protection of Sensitive but Unclassified Information," Section 4.3, dated March 2007, requires system owners to annually review the ISA and MOU agreements. Additionally, OCIO requires that ISA and MOU agreements are reviewed when a significant change occurs with the system.

Based on discussions with OCIO officials and a review of OCIO controls, we concluded that the deficiencies cited above were caused by the following:

- OCIO had not developed and implemented effective controls to ensure that system owners in conjunction with Perot Systems identified all internal and external connections to EDNIS.
- OCIO had not developed a process to identify all systems interfacing with EDUCATE that would enable the system owner to obtain the required documentation to support the various individual SSPs comprising EDUCATE.
- Although OCIO had established internal policies, it has not developed procedures to ensure that system owners annually review the ISA and MOU agreements with each system interface.
- OCIO and Perot Systems had not established effective procedures to obtain an accurate and complete inventory of systems interfacing with EDUCATE.
- OCIO did not have procedures to ensure that system owners perform re-accreditation and re-certification once every 3 years as required by OMB Circular A-130, Appendix III or on an annual basis for mission critical systems as required by OCIO-05, "Handbook for Information Technology Security Certification and Accreditation Procedures", dated March 2006.

Without adequate controls and procedures, the Department increases the security risks and vulnerabilities to EDUCATE that information transported and maintained may be subject to unauthorized activities. Those activities include the release of sensitive and personally identifiable information. Additionally, there is an increased risk that individual system security controls connecting to EDUCATE will be insufficient to meet the requirements of the highest security level based on ISA and MOU agreements. Further, without accurate information on the number of systems connecting to EDUCATE, vulnerabilities associated with the connecting systems will migrate to EDUCATE and thus jeopardize all the systems.

RECOMMENDATIONS:

We recommend OCIO:

- 8.1 Develop and implement effective controls to ensure that the EDNIS, EDMASS, CAMS, and EDSOC system owners in conjunction with Perot Systems identify all internal and external connections to these systems.
- 8.2 Develop a process to identify all systems interfacing with EDUCATE and provide the information to each of the system owners that comprise EDUCATE to enable them to obtain the required documentation to support the various individual system security plans.
- 8.3 Develop procedures to ensure that system owners annually review the ISA and MOU agreements for each system interface and update system security plans as necessary.
- 8.4 Develop automated tracking processes to ensure that system owners perform re-accreditation and re-certification as required every 3 years.
- 8.5 In conjunction with Perot Systems, establish and enhance procedures to obtain an accurate inventory of systems interfacing with EDUCATE.

Management Response

OCIO concurred with Recommendations 8.1, 8.2, 8.3, and 8.5. However, management did not concur with Recommendation 8.4. Management stated that the Department uses OVMS to track certifications and re-certifications. OCIO Information Assurance Services (IAS) is working with OVMS developers to create enhancements that will allow for the automated tracking of Department systems re-accreditation and re-certification. This enhancement is scheduled to be completed by March 31, 2012. OCIO IAS currently maintains a dashboard to monitor the certification and accreditation status of all systems within the Department. This dashboard includes a stoplight chart to provide indications and warnings to IAS and ISSOs when the system is getting close to or is out of compliance. The dashboard has only been used internally by IAS but is shared at the monthly ISSO meeting and quarterly IA Board of Directors meeting. Also, OCIO IAS has budgeted in fiscal years 2012 and 2013 to implement automated continuous security authorization in accordance with NIST and DHS guidance.

OIG Response

We reviewed management's response. OCIO reported that it uses automated tracking and monitoring tools such as OVMS and the IAS dashboard. Nonetheless, the audit found that systems still are not properly re-certified and re-accredited in accordance with OMB and NIST requirements. Thus, although the automatic tracking tools may identify needed re-accreditations and re-certifications, they are insufficient to ensure that system owners actually perform re-accreditation and re-certification as required. Therefore, OCIO needs to develop automatic

tracking processes to ensure that re-accreditations and re-certifications are performed as required. Therefore, the recommendation remains as stated.

9. Federal Desktop Core Configuration Security Configuration Management Process Needed Improvement

OMB Memorandum M-08-22, “Guidance on the Federal Desktop Core Configuration”, dated August 11, 2008, requires all Federal agencies standardize the mandated security configuration of approximately 300 settings on each of their desktops and laptops. Federal Desktop Core Configuration (FDCC) seeks to leverage configuration management by creating a standard for all Windows XP and Vista computers. According to OMB, the reason for this standardization is to strengthen Federal IT security by reducing opportunities for hackers to access and exploit government computer desktop systems. As part of the review, we conducted tests to determine whether OCIO had established sufficient security controls to comply with the FDCC requirements.

In 2010, OCIO reported 15 FDCC deviations in the OCIO Annual FISMA Report to OMB. We judgmentally selected two deviations to examine the authorization documents to support management’s decision to permit the deviations and found that OCIO was not able to locate the authorization documentation related to either deviation.

NIST SP 800-53, Revision 3, Appendix F, CM-6, “Configuration Settings” requires an agency to identify, document, and approve exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and to monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

OCIO had not established procedures to ensure that documentation supporting management’s decision to permit deviations to the standard FDCC is retained for audit. Although OMB and NIST guidance requires management to document deviations from FDCC standards, the EDUCATE SLA does not require justifying deviations that may be caused by hardware or software limitations.

Without the necessary supporting documentation for the deviation, OCIO cannot properly assess the deviation and its impact on the overall EDUCATE environment and cannot assess the associated risk presented by the deviation.

RECOMMENDATIONS:

We recommend OCIO:

- 9.1 Develop and implement procedures to ensure there is documentation supporting management’s decision to permit deviations to the standard FDCC. This documentation should be retained for audit, to demonstrate management’s decision making process authorizing the deviations to FDCC and to demonstrate its performance of key

monitoring responsibilities and compliance with OMB and NIST standards and requirements.

9.2 Require Perot to justify specific deviations that may be required by specific hardware or operating system software or application limitations.

Management Response

OCIO concurred with Recommendations 9.1 and 9.2.

10. The Department Needed to Update the Security Assessment and Authorization Documents

NIST in partnership with the Department of Defense, the Office of the Director of National Intelligence, and the Committee on National Security Systems has developed a common information security framework for the Federal government and its contractors. The intent of the common framework is to improve information security, strengthen risk management processes, and encourage reciprocity among Federal agencies. Authorizing officials make risk-based authorization decisions using the security authorization package, which includes key documents (security assessment and authorization documents) such as the systems security plan, the security assessment report, and the plan of actions and milestones.

OCIO and the system owners for CAMS, EDNIS, EDCAPS, and EDMASS should update their Security Assessment and Authorization documents. During our testing we identified the following deficiencies:

- The CAMS SSP was outdated and not compliant with OMB “Circular A-130 Appendix III” and NIST 800-53 Revision 3 requirements. The CAMS SSP, which should be updated annually, was last updated on May 14, 2008.
- The SSP’s Privacy Impact Assessments (PIA) for EDUCATE, EDNIS, and EDMASS are not in agreement. The EDUCATE PIA states that it does not process PII for EDNIS and EDMASS; however, the EDNIS and EDMASS plans state that they contain and process PII.
- The CAMS SSP is not compliant with NIST SP 800-18 “Guide for Developing Security Plans for Federal Information Systems”, Revision 1, dated February 2006, for documenting ongoing maintenance control system architecture, additions/deletions of system interconnections, and change in security authorization status.

OMB Memorandum 03-22 “OMB Guidance for Implementing the Privacy Provisions of the E-Government of 2002” states, “Agencies must update their PIA to reflect changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form.”

NIST SP 800-18, Revision 1, states that once the information system security plan is developed, it is important to periodically assess the plan, review any change in system status, functionality,

design, etc., and ensure that the plan continues to reflect the correct information about the system. This documentation and its correctness are critical for system certification activity. All plans should be reviewed and updated, if appropriate, at least annually.

Based on discussions with OCIO officials, System Security Officers (SSOs) and system owners did not ensure that procedures were properly developed to follow NIST SP 800-53, Revision 3 and 800-18, Revision 1 guidelines for updating the SSP for CAMS, EDNIS, EDMASS, and EDCAPS. Additionally, the Department's Privacy Office did not develop procedures to implement the OMB Memorandum 03-22 requirements for implementing and updating the EDUCATE and CAMS PIA. Further, OCIO internal operations do not assign responsibilities for reviewing OCIO policies and procedures as changes occur to the following NIST and OMB standards and requirements:

- to determine the need for changes to OCIO policies and procedures;
- to assess the impact on the Department's information security program; and
- to identify changes to the Department's information security program and OCIO policies and procedures.

We also found that the SSOs did not retain sufficient documentation to support the data sensitivity classification as part of the PIA assessment required for EDCAPS and CAMS SSPs.

Without an up-to-date SSP, system owners increase the risk that security controls may not be suitably designed to effectively secure sensitive data that are processed and maintained by the system. Additionally, Department management may not be aware of the risks introduced over time as a result of changes to the IT infrastructure and operational control. Further, inconsistent or improper assessment of the data sensitivity processed or maintained by a system increases the risks that PII data and other sensitive data will not be properly secured to prevent either unauthorized access to the data or prevent unauthorized release or use of PII data.

RECOMMENDATIONS:

We recommend OCIO:

- 10.1 Develop procedures to ensure that all SSPs follow OMB guidance and NIST SP 800-18, Revision 1, guidelines for updating the SSP to include the SSPs for CAMS, EDNIS, EDMASS, and EDCAPS.
- 10.2 Update OCIO-15 to ensure compliance with OMB Memorandum 03-22 guidelines for implementing and updating the EDUCATE and CAMS PIA.
- 10.3 Update OCIO-15 to bring it into compliance with NIST SP 800-53, Revision 3, Appendix F-PL, PL-1, Security Planning Policies and Procedures.
- 10.4 Develop procedures to ensure that the SSO retains sufficient documentation to support the required actions for the CAMS SSP.

Management Response

OCIO concurred with Recommendations 10.1 through 10.4. However, OCIO suggested that we revise Recommendation 10.4 to say “Develop procedures to ensure that the Information System Security Officer retains documentation used to complete Privacy Impact Assessments.”

OIG Response

Based on our review we do not believe there is a need to modify recommendation 10.4. Because a PIA is part of an SSP, retaining sufficient documentation for an SSP will include a PIA. OCIO stated that it agrees with the recommendation and will revise section 2.4 “Security Authorization Documentation” of the Security Authorization Guidance to include procedures that ensure System Security Officers retain the documentation used to complete the PIA. OCIO states the revisions to this guidance will be finalized by November 1, 2011.

11. Contingency Planning Program Needed Improvement

Based on our review of EDUCATE supporting documentation such as SSPs, risk assessments, Business Impact Analysis (BIA), Disaster Recovery Plans (DRP), Continuity of Operation Plans (COOP), and Business Contingency Plans (BCP), we noted the following deficiencies related to the contingency planning program:

- 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.
- OCIO, in conjunction with Perot Systems, had not developed contingency plans for EDNIS, EDMASS, CAMS, and EDSOC.
- 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.
- OCIO had not requested Telecommunication Service Priority (TSP) codes for National Security Emergency Preparedness as required by the DHS. 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. This condition was previously reported in fiscal year 2010 by the OIG in the audit report, Department of Education Virtual Data Center ED-OIG/A11J0006, dated September 2010.

Based on discussions with OCIO and Perot Systems officials and personnel, and our review of supporting documentation, we have concluded that the deficiencies resulted from the following:

1. OCIO management did not think that the BIA applied to its contingency planning process because it had developed an overall DRP for EDUCATE.
2. OCIO management felt that Perot Systems did not have to develop COOPs and BCPs for EDNIS, EDMASS, and EDSOC because the information was covered in the DRP.
3. OCIO stated that Perot Systems did not perform functional exercises on the individual systems because these systems were covered by the EDUCATE contingency plans.
4. OCIO personnel stated that they were only recently made aware of the TSP code issue but stated that the TSP codes will be established by December 2011.

NIST SP 800-53, Revision 3, requires agencies to develop contingency plans for major applications and general support systems to address recovery of the system in the event of a disaster or other significant disruption to service. Further, NIST SP 800-34, Revision 1, provides additional guidance to agencies in developing contingency plans to identify key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system. Additionally, SP 800-34, Revision 1, provides clarification and guidance on developing a contingency plan for information systems and general support systems based on an agency-wide risk assessment BIA. NIST SP 800-34 requires the agency to incorporate the BIA results into the analysis and strategy development efforts for the organization's COOP, BCP, and DRP documents.

OCIO-01, "Handbook for Information Assurance Security Policy," dated December 2005, and OCIO-13, "Handbook for Telecommunications," dated April 2006, restate the NIST requirements to develop and test contingency plans and to obtain TSP service.

Without the COOP, DRP, and BCP based on a BIA, the Department increases the risks that it will not recover mission critical functions based on established recovery priorities. Additionally, without the COOP, DRP, and BCP designed for each of the general support system comprising the EDUCATE environment, OCIO increases the risks that:

- Unique recovery requirements for these critical system operations will not be identified.
- Areas for improving the recovery process will not be identified without an annual test of the contingency plan at the system level.
- Corrective actions will not be initiated prior to an emergency, thus delaying or preventing recovery of systems supporting the Department's critical business functions.

Without TSP codes, OCIO cannot ensure that critical communications services are provided to Department senior management to enable them to carry out the Department's critical mission and functions in the event of a national disaster.

RECOMMENDATIONS:

We recommend OCIO:

- 11.1 Develop a BIA process and conduct a BIA on the EDUCATE Infrastructure.
- 11.2 Develop and maintain disaster recovery and contingency plans for EDUCATE's General Support Systems: EDMASS, EDNIS, CAMS, and EDSOC.
- 11.3 Require Perot Systems to perform functional exercises and full failover and failbacks on an annual basis for all of the EDUCATE infrastructure.
- 11.4 Develop and implement procedures and processes that ensure the requirements of the TSP Program for the EDUCATE are immediately met and ensure compliance with DHS requirements and OCIO-13, "Handbook for Telecommunications," and other applicable guidance.

Management Response

OCIO concurred with Recommendations 11.1, 11.3, and 11.4. However, management did not concur with Recommendation 11.2. In its response, OCIO stated that it has established contingency plans (CP), referred to as BCPs, and DRPs, for EDNIS, EDMASS, CAMS, and EDSOC.

OIG Response

We have reviewed management's response. For Recommendation 11.2, during the audit OCIO did not provide requested documentation relating to the CP, BCP, and DRP for EDNIS, EDMASS, CAMS, and EDSOC. We provided system owners and OCIO with sufficient opportunities to provide the required documentation to demonstrate compliance with NIST and OMB requirements. Therefore, Recommendation 11.2 remains as stated.

12. The Department Needed to Establish an Organization-Wide Risk Management Strategy

As part of our audit tests we reviewed the SSP associated with EDUCATE, EDNIS, EDMASS, EDSOC, and CAMS. Although OCIO and the system owners had performed application security risk assessments as part of the SSP, OCIO currently did not have an organization-wide risk management strategy as required by the OMB A-130 Appendices III and IV, and as clarified by the NIST SP 800-39, "Managing Information Security Risk", dated March 2011. The Director of OCIO Information Assurance (IA) stated that OCIO IA was currently in the process of developing an organization-wide risk management strategy.

Based on discussions with OCIO officials, OCIO had not developed processes and procedures to conduct risk assessments at the organizational level or system level because OCIO IA has not assigned the formal risk executive function to anyone.

NIST SP 800-39 states, “Risk management is a comprehensive process that requires organizations to: (i) frame risk (i.e., establish the context for risk-based decisions); (ii) assess risk; (iii) respond to risk once determined; and (iv) monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations. Risk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk based decision making is integrated into every aspect of the organization.”

Without an organization-wide risk management strategy, the Department increases the potential that known and unknown vulnerabilities will either not be identified or improperly categorized leading to exploitation of vulnerabilities and potentially compromising the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems.

RECOMMENDATIONS:

We recommend OCIO:

- 12.1 Develop and implement procedures to conduct risk assessments at the organizational level in addition to the currently performed application risk assessments.
- 12.2 Assess the potential impact on each application of any organization-wide security risk.
- 12.3 Enhance current risk assessment processes and procedures to incorporate the requirements of NIST SP 800-39.

Management Response

OCIO concurred with Recommendations 12.1 through 12.3. However, OCIO did not concur with Recommendation 12.4 which required OCIO to assign responsibility of the risk executive to an individual or group to coordinate with senior leadership of the Department the risk executive requirements outlined in NIST SP 800-39. In its response, OCIO stated that it has a Risk Executive that is the CIO and has assigned the Risk Management functions to the CISO. Additionally, the Director of IAS has developed an IA Strategic Plan that incorporates the requirements of NIST SP 800-39.

OIG Response

After reviewing management’s comments, we removed Recommendation 12.4 from the final report.

13. Documentation of Security Awareness Training Needed Improvement

OCIO policies require that newly hired personnel take security awareness training within 10 days of starting employment. Additionally, personnel with significant information security responsibilities (such as System Administrators) must take specialized training annually. Our review of the training records noted the following:

- OCIO could not provide supporting evidence for initial security awareness training for 22 of 25 newly hired personnel. Additionally, documentation for 3 personnel from the 25 showed that the employees did not attend training within the 10 day period.
- OCIO could not provide supporting evidence of training records for all 25 employees selected who had significant information security responsibilities.

NIST SP 800-53, Revision 3, Section Awareness Training (AT)-2, Security Awareness, requires agencies to establish and provide basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users and when required by system changes. Further, NIST SP 800-53 Revision 3, AT-4, Security Training Records recommends the agency retain individual training records. OCIO-01 requires employees to attend security training within 10 working days of employment and annually as a refresher.

The Department's process for capturing training information for contractor personnel does not require that individual training records be kept to support the actual training. The current process requires only that each Information System Security Officer (ISSO) keep track of attendees via an Excel spreadsheet.

Without an effective process for tracking employees and contractor personnel training, the Department increases the risks that employees are not made aware of security vulnerabilities and not adequately trained and educated on strong security practices to help reduce security vulnerabilities and risks.

RECOMMENDATIONS:

We recommend OCIO:

- 13.1 Develop procedures to ensure that all personnel provide documentation to the ISSO of training attended and to ensure the retention of the training documentation.
- 13.2 Enhance the ISSO tracking tool to include contractor personnel and to store the proof of completion for all users.

Management Response

OCIO partially concurred with Recommendations 13.1 and 13.2. For Recommendation 13.1, OCIO stated that NIST 800-53, Revision 3, AT-4, does not explicitly require agencies to retain

copies of training certificates as supporting documentation. NIST 800-53 does state that the Department's Talent Management System and Security Touch Learning Management System retain training completion data, and reports can be generated upon request. In addition, OCIO stated that procedures fully defining how documentation will be retained will be implemented by December 30, 2011.

For Recommendation 13.2, OCIO stated that OCIO IAS will issue a memorandum to the Department's Principal Offices requiring contractors to take annual awareness training using the public facing Security Touch learning management Web application for the FY 2012 training cycle. Security Touch will allow OCIO IAS to track and store proof of completion for all users. In instances where vendors use their own IT security training program or products to train their employees, OCIO will accept a certification letter from the company's authorized official that contains the list of employees who completed the training along with a description of the training provided.

OIG Response

We reviewed management's response. For Recommendation 13.1, if the document retention procedures that OCIO stated will be implemented by December 30, 2011 contain a provision for producing the documentation upon request, this corrective action should correct the deficiency cited.

For Recommendation 13.2, OCIO stated that Security Touch will allow OCIO IAS to track and store proof of completion for all users. Additionally, for those vendors who use their own IT security training program or products to train their employees, OCIO will accept a certification letter from the company's authorized official that contains the list of employees who completed the training along with a description of the training provided. Provided that both of these corrective actions are able to produce the training documentation upon request, these corrective actions should correct the deficiency cited. Therefore, upon further review and assessment of OCIO's responses, our recommendations will remain as stated, and OCIO will have an opportunity to proceed with the corrective actions proposed to resolve the recommendations.

14. Plan of Action and Milestones Process Was Not Adequately Managed

Plans of Action & Milestones (POA&M) are a management tool used to identify and manage security weaknesses. These plans are designed to be used largely by: (1) the CIO, program officials, and other appropriate agency officials to track progress of corrective actions; (2) the OIG to perform follow-up work with the agency; and (3) OMB to assist in its oversight responsibilities and to inform the budget process. OMB FISMA reporting requirements and Department guidance in the Department's POA&M Standard Operating Procedures (SOP), dated May 2010, requires that the Department's POA&M process include the type of weakness, responsible party for resolving the weakness, estimated funding resources required to resolve the weakness, scheduled completion date, key milestones with completion dates, milestone changes, source of the weakness, and status.

Based on our tests of the POA&M process and procedures, we identified the following issues that indicate that the POA&M process was not adequately managed:

- 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 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, OCIO did not provide management with all security weaknesses from its dashboard, specifically, contingency planning, annual assessment, certification and accreditation, and vulnerability scan findings.
- OCIO did not monitor all security weaknesses in the POA&M reports and audit dashboard. Currently, 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. OCIO Information Assurance team receives these monthly vulnerability scans from Perot Systems and then analyzes them before inputting the weaknesses into the POA&M OVMS database.

OCIO POA&M program is not compliant with OMB Circular A-130 Appendices III and IV. For the POA&Ms we reviewed, OCIO and program offices did not identify and report the security resources (i.e., tools and personnel/contractor hours) needed to remediate the security weaknesses and report the resources in the POA&Ms and on the OMB Exhibit 53 (Agency IT Investment Portfolio) and 300 exhibits (Capital Asset Plans and Business Cases).

The Department's POA&M SOP states that all findings or security weaknesses (including those identified as a significant deficiency or material weakness) must be included in and tracked on the POA&Ms. The SOP defines security system weaknesses resulting from:

- OIG Audits
- Risk Assessments
- Security Tests and Evaluations
- Penetration Tests
- Vulnerability Scans, and
- Government Accountability Office (GAO) Audits

Based on discussions with OCIO officials and review of documentation, we determined that scan results must go through a two-stage manual process before being entered into OVMS. OCIO personnel stated that the OVMS manual updates are behind schedule. Additionally, OCIO has not established a quarterly reporting deadline for the contractor to update the POA&M population. Further, OCIO stated that the system owners are responsible for updating the POA&Ms based on updated systems' security plans and re-accreditation of a system. However,

OCIO has not updated the POA&M standard operating procedures to provide guidance for linking resources needed to complete remediation to the OMB Exhibit 53 and Exhibit 300.

Without the proper review and maintenance of POA&M activities, Department management may not be aware of the security control weaknesses and the severity of weaknesses within various systems and the potential or actual impact of such weaknesses on other systems. Additionally, without adequate monitoring, management may be unaware of the status of corrective action and may not be able to assess and prioritize the resources needed to implement corrective actions. Further, OCIO lacks procedures to identify the resource requirements necessary to implement corrective action which increases the risks that insufficient resources will be made available to resolve the security control weakness in a timely manner.

RECOMMENDATIONS:

We recommend OCIO:

- 14.1 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.
- 14.2 Develop procedures to monitor the remediation of all actions within the POA&M population.
- 14.3 Develop procedures to estimate and record the resource requirements for implementing proposed corrective action in accordance with OMB Exhibits 53 and 300.
- 14.4 Develop an automated process to identify, track, maintain, and report security weaknesses resulting from the monthly vulnerability scans.

Management Response

OCIO concurred with Recommendations 14.1 through 14.4.

Appendix A: Objectives, Scope, and Methodology

To fulfill the OIG responsibilities related to FISMA to conduct a comprehensive and independent IT system security audit to determine the effectiveness of the Department's overall information security program and practices for the EDUCATE system the OIG contracted with Williams, Adley & Company LLP, (Williams Adley), to conduct an independent information security system audit of EDUCATE.

FISMA requires each Federal agency to develop, document, and implement an agency-wide information security program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Further, FISMA requires an annual assessment of the agency's security program to assess the adequacy and effectiveness of these controls. FISMA requires the agency inspector general, or an independent external auditor, to perform annual reviews of the information security program and to report those results to the OMB.

Additionally, FISMA delegates to OMB and the NIST the responsibility to develop information security regulations, requirements, and technical standards that all Federal agencies must implement in their information and information security program. FISMA, as well as OMB Circular A-130, "Management of Information Resources," Appendix III, "Security of Federal Automated Information Resources," requires an agency to develop sufficient controls to ensure that contractors providing IT services establish and maintain information and an information security program compliant with Federal laws, regulations, and standards. OCIO has the responsibility to ensure that the service provider for EDUCATE establishes and maintains information and information systems security controls that are compliant with Federal laws, regulations, and standards.

Objectives

Williams Adley conducted an independent evaluation of the effectiveness of OCIO's overall information security program and practices for the EDUCATE system. We also evaluated the level of compliance of information and information system security controls with Federal laws, regulations, and standards.

The audit was conducted in accordance with Government Auditing Standards, July 2007 Revision. 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.

We understand that the results of the detailed test work shall be incorporated into the OIG's annual independent evaluation of the Department's information security program and practices.

Scope

The scope of the audit included:

- The audit period of October 1, 2010 through April 30, 2011.
- An assessment of OCIO management oversight controls of the Perot Systems information security program for compliance with FISMA.
- An assessment of the Department's and Perot Systems' policies, procedures, and controls in place during the audit period against OMB Circulars A-130 "Management of Federal Information Resources" Appendix III "Security of Federal Automated Information Resources," A-127 "Financial Management Systems," and A-123 "Management Accountability and Control Sections III Assessing and Improving Management Controls, and Section IV Correcting Management Control Deficiencies"; and the NIST FIPS Publication Standards 199 – "Standards for Security Categorization of Federal Information and Information Systems," dated February 2004, and "200 Minimum Security Requirements for Federal Information and Information Systems," dated March 2006; and various NIST Special Publication (SP) Series 800 such as 800-53 version 3 "Recommended Security Controls for Federal Information Systems and Organizations," dated August 2009 and 800-53A "Guide for Assessing the Security Controls in Federal Information Systems," "Building Effective Security Assessment Plans", dated July 2008. Additional NIST Special Publications used in the evaluation included: SP 800-128 "Guide for Security Configuration Management of Information Systems" (Draft) dated March 2010; SP 800-63 Revision 1.0.2 "Electronic Authentication Guide" dated April 2006; SP 800-61, Revision 1, "Computer Security Incident Handling Guide," dated March 2008; SP 800-37 "Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems" dated February 2010; SP 800-30 Risk Management Guide for Information Technology Systems" dated July 2002; and SP 800-18 Revision 1 "Guide for Developing Security Plans for Information Systems" dated February 2006.
- An assessment of the effectiveness of the Department's management oversight controls as required by OMB Circular A-130, NIST FIPS Publication 200 and FISMA.
- A risk-based approach to selecting the key management, technical, and operational controls for testing from the NIST SP 800-53 control families and for testing a sample of key general and application controls as identified in the GAO's Federal Information Systems Control Audit Manual.
- Using a risk-based approach, we performed detailed security reviews of designated information systems and applications by conducting vulnerability assessments and limited penetration testing of EDUCATE. We tested to the levels that determined the adequacy of the Department's network security controls to prevent or detect unauthorized activities such as hackers. We also tested to determine the adequacy of the controls to identify and prevent viruses and other advanced persistent threats from entering the network and agency hardware. Before we conducted any tests, we obtained agreement from OCIO and OIG of the specific network vulnerability assessments software tools and penetration testing techniques and the nature and timing of the tests. This is commonly referred to as the "rules of engagement." We obtained a signed "rules of engagement" document from all parties.

- The audit location included testing at the Department’s headquarters in Washington, D.C., and the Perot Systems Data Center in Plano, Texas.

For the Network General Support System and for systems and applications residing on the EDUCATE network, we selected a representative sample of the EDUCATE subsystems: EDNIS, EDMASS, EDSOC, CAMS, EDCAPS.

The audit program covered at a minimum the following NIST management, operational, and, technical controls.

Management Control

1. NIST SP 800-37 Revision 1 “Guide For Applying The Risk Management Framework To Federal Information Systems” (documentation, process review, requirements, and re-certifications)
2. Risk Assessment (periodic reviews, categories, and magnitude of harm)

Operational Controls

1. Security Awareness and Training (rules of behavior, annual training, and specialized training)
2. Configuration Management (life cycle methodology, documented policy, access restrictions, current inventory, and proper configuration plan)
3. Contingency Planning (properly documented contingency plan, testing the plan, assigned individuals, and alternate processing site)
4. Incident Response and Handling (interconnection agreements, user support, annual training, and capability tests)
5. Media Protection (labeling, storing, physical security controls, protection, only authorized access, approvals)
6. Physical and Environmental Protection (protection commensurate with risk, fire suppression, fences, granting physical access, monitoring, and review of visitor logs)
7. Personnel Security (least privilege, individual accountability, and background screenings)

Technical Controls

1. Access Controls (least privilege, user roles, segregation of duties, termination of accounts, password conformity, and appropriate agreements)
2. Audit and Accountability (virus protection, integrity and validation controls, authenticated passwords, and logical access controls)
3. Personal Identifiable Information (safeguarded, and need to know)

Network Vulnerability and Penetration Testing

1. Using a risk-based approach, we performed detailed security reviews of designated information systems and applications by conducting vulnerability assessments and limited penetration testing.
2. We tested to the levels that determined the effectiveness of the Perot Systems controls to protect and secure Department data and to prevent potential advanced and persistent threats to the Department's network architecture.

Appendix B: Office of Chief Information Officer Comments



UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF THE CHIEF INFORMATION OFFICER

THE CHIEF INFORMATION OFFICER

MEMORANDUM

SEP 8 2011

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

FROM: Danny A. Harris, Ph.D. 

SUBJECT: Draft Audit Report
Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) Information Security Audit
Control Number ED-OIG/A11L0001

Thank you for the opportunity to comment on the draft Office of Inspector General's (OIG) report, Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) Information Security Audit Control Number ED-OIG/A11L0001. Your draft audit report provides insight into the effectiveness of the information systems security controls in place to secure the EDUCATE environment, and accurately identifies several areas of needed improvement. The Office of the Chief Information Officer (OCIO) sincerely appreciates the attention provided by this report and looks forward to working with your office to appropriately address the recommendations. However, it is also important to note that many of the substantive and quantifiable process improvements implemented during the course of the audit demonstrate significant improvement in the information system security controls pertaining to the EDUCATE environment.

OCIO will address each finding and recommendation as stipulated in the plan provided, and as agreed upon by your office.

Security Configuration Management Process Needed Improvement

Prior to the issuance of the draft report, OCIO Information Assurance Services (IAS) had developed baseline configuration guidelines for each operating system and enterprise-wide applications in the EDUCATE environment based on the Department of Defense Security Technical Implementation Guidelines (STIGs). As changes are made to the system, due to security patches and/or bug fixes, the baseline configurations shall be updated, specific configuration settings confirmed, and configuration items tracked, verified and reported.

On August 26, 2011, the Department's Chief Information Security Officer (CISO) issued a memorandum to Del. Systems (formerly known as "Perot Systems") Information Technology (IT) Security Manager requiring that all Department devices be configured to the newly established baseline settings and periodically checked to ensure compliance.

400 MARLAND AVE. S.W., WASHINGTON, DC 20202
www.ed.gov

The Department of Education's mission is to promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access.

OIG Recommendation 1.1 “Revise the SLA to require Dell Systems to take appropriate timely corrective action to resolve network security configuration vulnerabilities or justify not implementing suggested corrective action to permit OCIO to assess the potential effect of the vulnerability versus the costs associated with implementing the suggested corrective action.”

Management Response: OCIO concurs with this recommendation. OCIO will enter into negotiations with Dell Systems to revise Service Level Agreement (SLA) “SP-7, Enterprise Vulnerability Management Service” to include performance standards to ensure configuration vulnerabilities identified during monthly scans are remediated within the time period established in the Department’s Vulnerability and Patch Management Guidance. OCIO IAS will submit the proposed SLA revisions to the EDUCATE Contracting Office Representative (COR) by December 1, 2011.

OIG Recommendation 1.2 “Revise the SLA to require Dell Systems to use various scanning software such as STIG automated tools that are compliant with National Institute of Standards and Technology (NIST) SP 800-128 (draft) to identify security vulnerabilities with configuration settings for clients and servers, databases, and network infrastructure devices (firewalls, routers, and switches) supporting EDUCATE.”

OCIO suggests changing this recommendation to: Develop and implement policies and procedures which require the use of a Security Content Automation Protocol (SCAP) compliant tool to identify security vulnerabilities with configuration settings within the operating systems for clients and servers, databases, and network infrastructure devices (firewalls, routers, and switches) supporting EDUCATE.

Rationale: The Department is not federally mandated to comply with Defense Information Systems Agency (DISA) STIGs. However, the DISA STIGs are a good beginning to baseline and the Department is employing them, as well as NIST automated SCAP compliance tools, to validate configurations.

Also, NIST and the federal government are moving to automated SCAP compliance tools to continuously monitor security vulnerabilities and configurations.

Management Response: OCIO concurs with this recommendation. Dell Systems currently conducts regular scanning using FoundStone scanning tools and Federal Desktop Core Configuration (FDCC) scanners. Additionally, the U.S. Department of Education’s Computer Incident Response Capability (EDCIRC) has purchased and is implementing Core Impact for network scanning.

To address automated Continuous Monitoring (CM) of vulnerabilities and configurations, OCIO IAS is deploying the RedSea change detector tool, using configuration files from EDUCATE and Federal Student Aid’s (FSA) Virtual Data Center (VDC). This tool will be utilized to generate an intuitive, network map that shows access paths throughout the network, attack paths based on inadequate network configuration, and vulnerability correlation. As the RedSea project evolves, it will become one of the centerpieces of the Continuous Monitoring Program (CMP).

through tracking and approving changes to the network's devices designed to resolve network security configuration vulnerabilities and ensuring compliance to baseline security configurations. RedSeal will be fully deployed by January 15, 2012.

Network Security Controls over Hardware Devices Needed Improvement

OIG Recommendation 2.1 Develop and implement policies and procedures to fully account for software or hardware installed or permitted to be used on the EDUCATE network.

OCIO suggests changing this recommendation to: Develop and implement policies and procedures to fully account for software or hardware installed on the EDUCATE network.

Rationale: The Department's Enterprise Architecture Review Board (EARB) maintains an End User Catalog of software and hardware that are permitted to be installed on the EDUCATE network. This procedure is captured in the Department's Enterprise Architecture Review Board Guidance.

Management Response: OCIO concurs with this recommendation. OCIO has implemented procedures to account for all software and hardware on the EDUCATE network. Dell Systems performs monthly scans of all devices on the network and compares it against the Configuration Management Database (CMDB) for discrepancies. Devices that are not listed in the CMDB are classified as rogue. Rogue devices are subject to Security Incidents (SLA SP-1, "Event/Incident Notification") reporting and isolation from the network (SLA SP-2, "Incident Containment"). OCIO Information Technology Services (ITS) will document the procedures followed to resolve reporting variances, such as undetermined operating systems and unknown host names by February 1, 2012. Additionally, OCIO IAS has begun engineering analysis to pilot network access control (NAC) software which is scheduled to be fully implemented by the end of Fiscal Year (FY) 2012.

OIG Recommendation 2.2 Revise the SLA requirements to require Dell Systems to implement procedures to carry out its responsibility for ensuring that only authorized devices are permitted to be installed on the network and to verify the number of devices permitted on the EDUCATE network or to obtain a reliable accountability of hardware.

Management Response: OCIO concurs with this recommendation. OCIO will enter into negotiations with Dell Systems to revise SLA "SP-6, Enterprise End User Devices Security Version", to implement metrics to ensure Dell Systems carries out their responsibility for verifying that only authorized devices are permitted to be installed on the network and to verify the number of devices permitted on the EDUCATE network or to obtain a reliable accounting of hardware. OCIO IAS will submit the proposed SLA revisions to the EDUCATE OOR by December 1, 2011.

OIG Recommendation 2.3 Require Dell Systems to resolve the monthly reporting variances, such as undetermined operating systems and unknown host name within 5 working days.

Management Response: OCIO concurs with this recommendation and this action has been completed. OCIO IAS had an independent assessment of the EDUCATE network (IA Discovery Project) performed during FY11 which resulted in a full report of devices with undetermined Operating Systems (OS) and host names. Operational Process Applications Suite (OPAS), the Dell Systems-proprietary version of Remedy Ticket System, tickets have been opened to address these findings. Additionally, the CISO has issued a memorandum directing Dell Systems to resolve the monthly reporting variances, such as undetermined operating systems and unknown host names within five working days.

OIG Recommendation 2.4 Require Dell Systems to terminate the network connections and authorizations for hardware labeled as "undetermined."

Management Response: OCIO concurs with this recommendation, action completed. The Department CISO has issued a memorandum directing Dell Systems to terminate the network connections for hardware identified as "undetermined" during the IA Discovery Project.

Security Patch Management Process Needs Improvement

OIG Recommendation 3.1 Amend the SLA to establish detailed performance reporting factors that would disclose the number of security patches released by vendors within the past reporting period, the criticality of the security patch, the number of network devices affected by the security patch, the number of devices patched, and the number of devices remaining to be patched.

Management Response: OCIO concurs with this recommendation. OCIO will enter into negotiations with Dell Systems to revise an existing SLA to manage the patching of enterprise wide applications and devices.

OCIO will enter into negotiations with Dell Systems to revise SLA "SP-8 Security Patching Windows" to establish detailed performance reporting factors that will disclose the number of security patches released by vendors within the past reporting period, the criticality of the security patch, the number of network devices affected by the security patch, the number of devices patched, and the number of devices remaining to be patched. OCIO IAS will submit the proposed SLA revisions to the EDUCATE COR by December 1, 2011.

OIG Recommendation 3.2 Amend the SLA to include language such as "the contractor must initiate the installation of vendor security patches within a 3-day period from the vendor release date or provide OCIO with a justification for not installing the security patch."

Management Response: OCIO concurs with this recommendation. The Department will enter into negotiations with Dell Systems to revise SLA "SP-8 Security Patching Windows" performance standard to require Dell Systems to initiate the installation of critical security patches within a 3-day period from the vendor release date or provide OCIO with a justification

for not installing the security patch. OCIO IAS will submit the proposed SLA revisions to the EDUCATE COR by December 1, 2011.

OIG Recommendation 3.3 Require Dell Systems to report monthly on the security patches received by the vendor but not installed during the period and include a schedule for installing the patch.

Management Response: OCIO concurs with this recommendation. The Department will revise the Vulnerability and Patch Management Guidance to include procedures for Dell Systems to report monthly on the security patches received by the vendor but not installed during the period established in SLA "SP-8 Security Patching Windows" and include a schedule for installing the patch. The Department CISO has issued a memorandum requiring Dell Systems to submit a Risk Acceptance Form (RAF) for missing patches and identified vulnerabilities on a monthly basis. These RAFs will be submitted to CISO for approval. The Patch Management Guidance will be revised by October 31, 2011.

Remote Access Software Was Not Compliant with OMB and NIST Standards

OIG Recommendation 4.1 Require Dell Systems to change the digital certificate and bit encryption for remote servers to the recommended settings that are specified in NIST 800-57 Part 3.

Management Response: OCIO concurs with this recommendation. Dell Systems is aware of the issue and is researching how to best comply with NIST SP 800-57, "Recommendation for Key Requirements Part 3: Application-Specific Key Management Guidance", requirements. OCIO Information Technology Service (ITS) will submit a plan for implementing NIST 800-57 Part 3 guidance by February 2012.

OIG Recommendation 4.2 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 (09-220005), Control Number L21K0022.

Management Response: OCIO concurs with this recommendation. The Department and Federal Student Aid (FSA) have used the intervening time since the issuance of the Investigative Program Advisory Report (IPAR) - Weakness in the Process for Handling Compromised Privileged Accounts" (09-220005), Control Number L21K0022, to acquire staff, refine action plans, secure funding and approval to address the issues cited in the report. OCIO has been working diligently on Personal Identity Verification (PIV) card deployment and has a documented strategy for two-factor authentication for both Government Funded Equipment (GFE) and non-GFE which will assist in the closure of the final open recommendation by the current November 2012 due date.

Dell Systems Network Operating System Controls for Identifying and Resolving Vulnerabilities Needed Improvement

OIG Recommendation 5.1 Direct Dell Systems to take immediate action to address the vulnerabilities identified and report to OCIO on the schedule for implementing the remedial action.

Management Response: OCIO concurs with this recommendation. The review of vulnerabilities identified by the OIG was completed on July 29, 2011. Based on the findings identified in the audit report, the Department will develop a timetable for complete remediation by October 15, 2011. The Department will take immediate corrective action on all identified critical vulnerabilities.

OIG Recommendation 5.2 Direct Dell Systems to enhance its current operating procedures to perform network scans every two weeks or more frequently as necessary.

OCIO suggests changing this recommendation to: OCIO should direct the vendor to enhance current operating procedures to perform network scans every two weeks or more frequently as necessary.

Rationale: This action should be assigned to the Department for remediation.

Management Response: The Department concurs with this recommendation. The Department is fully committed to meeting Office of Management and Budget's (OMB) requirements for maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions, as detailed in Memorandum M-11-29. The Department is in the final stages of awarding a task order to acquire a CM data collection tool and provide OCIO IAS assistance with services that support the development of an architecture capability to provide automated CM of all of the Department's networks in accordance with OMB Memorandum M-10-15 FY 2010, NIST Special Publication (SP) 800-27, and NIST SP 800-127. The vendor selected to perform this task will be responsible for recommending an enterprise solution that most meets government requirements and industry best practices (Continuous Asset Evaluation, Situation Awareness, and Risk Scoring (CAESARS) Reference Architecture). The current target date for deploying this CM tool is December 30, 2011.

The Department's Incident Response Program Needed Improvement to Ensure Timely and Appropriate Detection, Reporting, and Resolution of Computer Security Incidents to Internal and External Parties

OIG Recommendation 6.1 Dell Systems to comply with the EDUCATE SLA for resolving incidents within the SLA specified timeframe.

Management Response: OCIO concurs with this recommendation. OCIO IAS has hired a new Chief of Cyber Operations who manages and oversees the EDCIRC and the Incident Response

Program: OCIO IAS has already begun measures to improve Dell Systems's compliance with the SLA to include business process improvements efforts, EDUCATE Network Information System incident response action plan reviews, and formal guidance communications. OCIO IAS expects continued improvement in this area.

OIG Recommendation 6.2 Dell Systems to implement recommendations cited in the Investigative Program Advisory Report – Incident Response and Reporting Procedures (10-1103832) control number L21L0001.

Management Response: OCIO concurs with this recommendation. As noted in the response memorandum cited, "Investigative Program Advisory Report Incident Response and Reporting Procedures (10-1103832) Control Number L21L0001", that (NAC) submitted to OIG on August 16, 2011, OCIO IAS is in the process of implementing the following changes to improve the Department's incident response and reporting activities:

- OCIO IAS will publish an incident responder guide that will clearly delineate roles and responsibilities of the Department employees and contractors in relationship to the incident's involvement in a computer-related incident by December 1, 2011.

OCIO IAS will deploy three additional network sensors to cover both the EDUCATE and Virtual Data Center (VDC) Demilitarized Zones (DMZ). Additional network sensors will be placed within ED.gov architecture at ADP. All sensors will be deployed by November 1, 2011.

- OCIO IAS will install DrCose Enterprise software and dedicated hardware to enable quicker incident response capabilities for gathering live forensic data. FBI/DOJ personnel will receive training on this capability. DrCose installation is scheduled for implementation by October 15, 2011.

Access and Identity Management Processes Required Significant Improvement

OIG Recommendation 7.1 Ensure that Active Directory is routinely reviewed for access privileges of users.

Management Response: OCIO concurs with this recommendation. OCIO IAS is leading an Active Directory "clean up" project which will provide a complete review of privileged access within the EDUCATE environment.

IAS currently maintains a list of individuals with temporary and permanent privileged access. The EDUCATE Information System Security Officer (ISSO) will review and check this list against the Active Directory (AD) on a quarterly basis beginning the first quarter of FY12.

OIG Recommendation 7.2 Configure the Active Directory account management automated tools to flag accounts that have not been used and ensure that all accounts are configured with passwords that have an expiration date.

Management Response: OCIO concurs with this recommendation and has initiated corrective action. On August 1, 2011, Dell Systems 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 (EDU.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.

In addition, OCIO will work with Dell Systems to implement additional procedures to ensure all Active Directory accounts have an expiration date which aligns with the Department's Password Security Guideline, unless specifically approved for an exception via a RAB. The procedure will be implemented by December 30, 2011.

OIG Recommendation 7.3 Revise the SLA to include a performance incentive or penalty clause to enforce OCIO account management policies such as disabling inactive accounts and terminating accounts of separated employees.

Management Response: OCIO concurs with this recommendation. OCIO will propose revisions to SLA HD-1 "Disable User Accounts", to require the disabling of accounts that have been inactive for over 90 days.

OCIO will negotiate with Dell Systems to make revisions to HD-1 to include a penalty clause to enforce OCIO account management policies which require terminating accounts of separated employees within one hour of notification from the Department. OCIO IAS will submit the proposed SLA revisions to the EDUCATE COR by December 1, 2011.

EDUCATE Network Information System (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

OIG Recommendation 8.1 Develop and implement effective controls to ensure that the EDNIS, EDMASS, CAMS, and EDSOC system owners in conjunction with Dell Systems identify all internal and external connections to these systems.

Management Response: OCIO concurs with this recommendation. Identification of internal and external connections is part of the Risk Management Framework (RMF) built into NIST 800-17 and NIST 800-53 which the Department follows. The CISO has established a certification and accreditation (C&A) Tiger Team to conduct a program review of the current C&A program and make recommendations to improve Risk Management business processes at the network and application layers.

Additionally, through the continuous monitoring program and the implementation of the RedSeal tool, the EDCIRC will have visibility of the internal and external connections. As previously stated, the RedSeal tool is currently in pilot with Initial Operating Capabilities (IOC) scheduled for first quarter FY 12.

OIG Recommendation 8.2 Develop a process to identify all systems interfacing with EDUCATE and provide the information to each of the system owners that comprise EDUCATE to enable them to obtain the required documentation to support the various individual system security plans.

Management Response: OCIO concurs with this recommendation. OCIO IAS is working with ITS and Dell Systems to develop a Security Requirements Traceability Matrix (SRTM) to facilitate system owner and ISSO visibility regarding security controls which can be inherited from EDUCATE as the general support system and what risks are being accepted by the General Support System (GSS) to support them in making informed design and risk decisions. A basic SRTM will be completed by January 30, 2012. EDUCATE will be going through the triennial C&A process during FY 12 which will enable greater detail to be analyzed and documented.

OIG Recommendation 8.3 Develop procedures to ensure that system owners annually review the ISA and MOU with each system interface and update system security plans as necessary.

Management Response: OCIO concurs with this recommendation. OCIO IAS will revise section 2.4, "Security Authorization Documentation" of the Security Authorization Guidance to include procedures which ensure System Owners (SO) annually reviews the Inter-Agency Service Agreement (ISA) and Memorandum of Understanding (MOU) with each system interface and to update system security plans as necessary. The revised guidance will be finalized by November 1, 2011. This requirement will be communicated to Department ISSOs at the 1st Quarter FY 12 ISSO meeting.

OIG Recommendation 8.4 Develop automated tracking processes to ensure that system owners perform recertification and re-certification as required every three years.

Management Response: OCIO non-concurs with this finding. The Department uses Operational Vulnerability Management Solution (OVMS) to track certifications and recertifications. OCIO IAS is working with OVMS developers to create enhancements which will allow for the automated tracking of Department systems recertification and recertification. This enhancement is scheduled to be completed by March 31, 2012.

OCIO IAS currently maintains a dashboard to monitor the C&A status of all systems within the Department. This dashboard includes a spotlight chart to provide indications and warnings to IAS and ISSOs when the system is getting close to or is out of compliance. This dashboard has only been utilized internal to IAS but is shared at the monthly ISSO meeting and quarterly IA Board of Directors meeting.

Also, OCIO IAS has budgeted in FY12 and FY13 to implement automated continuous security authorization in accordance with NIST and Department of Homeland Security (DHS) guidance.

OIG Recommendation 8.5 In conjunction with Dell Systems, establish and enhance procedures to obtain an accurate inventory of systems interfacing with EDUCATE.

Management Response: OCIO concurs with this recommendation. OCIO IAS is developing and implementing procedures to obtain an accurate inventory of systems interfacing with EDUCATE using the RedSeal network mapping tool and Discovery tool currently in pilot.

Federal Desktop Core Configuration Security Configuration Management Process Needs Improvement

OIG Recommendation 9.1 Develop and implement procedures to ensure there is documentation supporting management's decision to permit deviations to the standard FDCC. This documentation should be retained for audit, to demonstrate management's decision making process to authorize the deviations to FDCC and to demonstrate its performance of key monitoring responsibilities and compliance with OMB and NIST standards and requirements.

Management Response: OCIO concurs with this recommendation. OCIO will revise the Plan of Actions and Milestones (POA&M) Guidance to include procedures for capturing the approval of Federal Desktop Core Configuration (FDCC) deviations. Dell Systems will be required to submit business justification for all FDCC deviations to the EARB for approval. If a deviation is deemed feasible a RAF will be submitted to OCIO IAS for final approval. These procedures will ensure the documentation capturing deviation approvals are properly retained for future audits, to demonstrate management's decision making process to authorize the deviations to FDCC and to demonstrate its performance of key monitoring responsibilities and compliance with OMB and NIST standards and requirements. The finalized procedure will be published by January 10, 2012.

OIG Recommendation 9.2 Require Dell Systems to justify specific deviations that may be required by specific hardware or operating system software or application limitations.

Management Response: OCIO concurs with this recommendation, action completed. The Department's CISO has issued a memorandum to Dell Systems requiring them to submit a RAF for each FDCC deviation identified by ITS. These RAFs will be subject to the Department's CISO approval.

The Department Needed to Update the Security Assessment and Authorization Documents

OIG Recommendation 11.1 Develop procedures to ensure that all SSPs follow OMB guidance and NIST 800-18, Revision 1, guidelines for updating the SSP to include the SSPs for CAMS, EDNIS, FDMASS, and EDUCAPS.

Management Response: OCIO concurs with this recommendation. Section 5.5.1, "Quarterly Documentation Review" of OCIO's Security Authorization Guidance, which was published on June 9, 2011, specifies the periodicity for updating all Department System Security Plans as being quarterly and/or whenever there is a significant change to the IT systems or to the interconnection. This requirement will be re-emphasized to Department ISSO's during the 4th Quarter ISSO meeting and provided to the IA Board of Directors by the 1st Quarter FY 12.

OIG Recommendation 10.2 Update OCIO-15 to ensure compliance with OMB Memorandum 03-22 guidelines for implementing and updating the EDUCATE and CAMS PIA.

Management Response: OCIO concurs with this recommendation. On February 8, 2011, the Office of Management (OM) established a Controlled Unclassified Information (CUI) Working Group to ensure the Department's compliance with federal mandates including Executive Order 13526 "Controlled Unclassified Information" and OMB Memorandum 03-22, "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002". In coordination with the OM, OCIO IAS will submit revisions to OCIO-15 to Administrative Communication Services team for final approval by the 2nd quarter FY 12.

OIG Recommendation 10.3 Update OCIO-15 to bring it into compliance with NIST 800-57, Revision 3, Appendix FPI, FPI-1, Security Planning Policies and Procedures.

Management Response: OCIO concurs with this recommendation. In coordination with OM, OCIO IAS will update the Information System Security section of OCIO-15 to include the Department's security planning procedures. The revisions to this directive will be finalized by November 1, 2012.

OIG Recommendation 10.4 Develop procedures to ensure that the SSO retains sufficient documentation to support the requirements for the CAMS SSP.

OCIO suggests changing this recommendation to: Develop procedures to ensure that the Information System Security Office retains documentation used to complete Privacy Impact Assessments.

Rationale: The revised recommendation specifically captures the essence of the deficiency noted in the audit report, which addresses privacy.

Management Response: OCIO concurs with this recommendation. OCIO IAS will revise section 2.4, "Security Authorization Documentation" of the Security Authorization Guidance to include procedures which ensure System Security Officers retain the documentation used to complete the Privacy Impact Assessment. The revisions to this guidance will be finalized by November 1, 2011.

Contingency Planning Program Needed Improvement

OIG Recommendation 11.1 Develop a BIA process and conduct a BIA on the EDUCATE Infrastructure.

Management Response: OCIO concurs with this recommendation. OCIO ITS has developed a Business Impact Analysis (BIA) Management Plan and BIA Template based on NIST 800-34, "Contingency Planning Guide for Federal Information Systems", which will be finalized by September 15, 2011. The project plan to conduct an enterprise-wide BIA will be initiated on September 16, 2011. OCIO will conduct NIST 800-34 based BIA according to management and project plans going forward. OCIO ITS will update procedures to require a BIA be conducted on an annual basis for all Federal Information Security Management Act (FISMA) reportable systems.

OIG Recommendation 11.2 Develop and maintain disaster recovery and contingency plans for EDUCATE's General Support Systems: EDMASS, EDNIS, CAMS, and EDSOC.

Management Response: OCIO non-concurs with this recommendation. OCIO has established contingency plans, referred to as Business Continuity Plans (BCP), and Disaster Recovery Plans (DRP) for EDNIS, EDMASS, CAMS, and EDSOC.

OIG Recommendation 11.3 Require Dell Systems to perform functional exercises and full fail-over and fail-backs on an annual basis for all of the EDUCATE infrastructure.

Management Response: OCIO concurs with this recommendation, action completed. On May 14-15, OCIO ITS conducted the full functional annual test of the Florence Technology Center (FTC). The test results were finalized and added to the EDUCATE C&A package on June 16, 2011.

OIG Recommendation 11.4 Develop and implement procedures and processes that ensure the requirements of the Telecommunication Service Priority (TSP) Program for the EDUCATE are immediately met and ensure compliance with Department of Homeland Security (DHS) requirements and OCIO-13, "Handbook for Telecommunications," and other applicable guidance.

Management Response: OCIO concurs with this recommendation. OCIO 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.

The Department Needs to Establish an Organization-Wide Risk Management Strategy

OIG Recommendation 12.1 Develop and implement procedures to conduct risk assessments at the organizational level in addition to the currently performed application risk assessments.

Management Response: OCIO concurs with this recommendation. The Director of IAS has developed an IA Strategic Plan that builds from all three perspectives of the Risk Management Framework (RMF) established in NIST 800-37 Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach". Goal One addresses governance and Goal's Two, and Three address both business and information systems risks. The plan incorporates a strong portfolio management approach with a federated enterprise governance structure to ensure the most critical risks are reviewed, accepted, and maintained appropriately for the Department's risk tolerance. Through the IA Strategic Plan, the maturity levels will continue to become more robust.

Tier 1's goal is to establish an effective method to conduct risk assessment at the organizational level. Risk Management from an organizational perspective has been the least mature element within the IA Framework. Recognizing this gap the CIO has taken a number of proactive steps to build and mature this risk function:

- Hired a SES-level Chief Information System Security Officer (CISO) to oversee the IA Program and provide strategic guidance for information assurance, cyber security, and risk management.
- In partnership with key Department Senior Leaders, established the IA Board of Directors in December 2010. The function of this chartered governance body is to guide and direct the Agency-wide risk management strategy, provide risk mitigation guidance, and set the risk tolerance for the Department. The IA Board of Directors meets bi-monthly. It continues to grow in maturity as the IA Strategic Plan is implemented and as risk and threat issues are turned and brought to the forefront.
- The CISO has initiated a Department-wide Security Architecture Working Group which assesses enterprise security capabilities. This working group is developing the Department of Education Enterprise Security Architecture.

Future phases in enhancing Tier 1 Organizational Risk Management include developing operational metrics to measure risk and present to the IA Board of Directors, implementing an automated Risk Scoring system, such as the Department of State's iPower tool, within the Department. The Department will implement an automated Risk Scoring capability by February 1, 2012.

OIG Recommendation 12.2 Assess the potential impact on each application of any organization wide security risk.

Management Response: OCIO concurs with this recommendation. In support of the continuous security authorization, the Department is developing and implementing a CM

capability that will provide a near real time capability to assess the effectiveness and functioning of numerous technical security controls, making it possible to assess system risk on a more frequent basis, which will strengthen and enhance the system's operational security posture. The Department will finalize the implementation of the framework established in NIST 800-37 by January 15, 2012.

OIG Recommendation 12.3 Enhance current risk assessment processes and procedures to incorporate the requirements of NIST SP 800-39.

Management Response: OCIO concurs with this recommendation. OCIO IAS will revise an organization-wide risk management strategy to ensure that our Risk Assessment processes are fully defined and implemented by December 30, 2011.

OIG Recommendation 12.4 Assign responsibility of the risk executive to an individual or group to coordinate with senior leadership of the Department the risk executive requirements outlined in NIST SP 800-39.

Management Response: OCIO non-concurs with this recommendation. Within the Department, the Risk Executive, as defined by NIST SP 800-39, *Managing Risk from Information Systems*, Apr 2008, is the CIO and the function is executed by the CISO. The Department recognizes the significant and growing danger of cyber threats and the necessity for leaders at all levels of an organization to understand their responsibilities for achieving adequate information security and for managing information system-related security risks.

"The NIST Risk Management Framework (RMF) emphasizes: (i) building information security capabilities into federal information systems through the application of state-of-the-practice management, operations, and technical security controls; (ii) maintaining awareness of the security state of information systems on an ongoing basis through enhanced monitoring processes; and (iii) providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the operation and use of information systems."

The Director of IAS has developed an IA Strategic plan (Figure 1) that builds from all three perspectives; Goal 1 addresses governance and Goals 2 and 3 address both business and information systems risks. The plan incorporates a strong portfolio management approach with a federated enterprise governance structure to ensure the most critical risks are reviewed, accepted, and mitigated appropriately for the Department's risk tolerance.

Figure 1: IA Strategic Plan 2011-2015

Goal 1: Organize for Unity of Purpose	Goal 2: Design for a Secure Enterprise	Goal 3: Build a strong network defense capability
<ul style="list-style-type: none"> 1.1 Lead and govern in a dynamic IT environment <ul style="list-style-type: none"> Set an enterprise direction Foster a culture of accountability relative to resources and risk Enhance the Risk Management Framework Provide guidance and oversight across the Department 1.2 Partner for strength <ul style="list-style-type: none"> Intra-Department Intra-government Academia IT and Cybersecurity industries 1.3 Develop the IA Workforce <ul style="list-style-type: none"> Educate and train the IA workforce Structure the workforce 	<ul style="list-style-type: none"> 2.1 Enhance our Risk Management framework <ul style="list-style-type: none"> 2.2 Design security into systems up front <ul style="list-style-type: none"> Incorporate Security from the beginning into architecture Incorporate Systems Security into the system development lifecycle Focus priorities on the future Balance risk 2.3 Design and implement an Integrated Identity management system to support the enterprise <ul style="list-style-type: none"> ITSP-A-12 Compliance Interior Identity Management 2.4 Establish an Enterprise Network Defense Architecture <ul style="list-style-type: none"> Situation Awareness Platform Sensor architecture Vulnerability Mgmt. Automated Configuration Mgmt. Correlation tools 	<ul style="list-style-type: none"> 3.1 Establish a network defense framework <ul style="list-style-type: none"> Tier 1-OTC/OT Tier 2-EC/CNC Tier 3-IT Service Provider SOC 3.2 Understand our network environment <ul style="list-style-type: none"> Know our networks (logically and physically) Know our threat factors and our risk gaps Understand the effects of malicious cyber actions 3.3 Prevent or delay attackers from getting in <ul style="list-style-type: none"> Defend the perimeter Secure hosts and networks Continuously assess perimeter and access points 3.4 Prevent an attacker from maintaining access <ul style="list-style-type: none"> Rapidly detect, diagnose and respond Contain privileged access Limit freedom to move through the enterprise

Documentation of Security Awareness Training Needs Improvement

OIG Recommendation 13.1 Develop procedures to ensure that all personnel are required to provide documentation to the ISSO of training attended and to ensure the retention of the training documentation.

Management Response: OCIO partially concurs with this recommendation. NIST 800-53 Revision 3, AT-4, does not explicitly require agencies to retain copies of training certificates as supporting documentation. During the course of the audit, OCIO was specifically asked to provide copies of the training awareness certificates for the employees selected for security awareness training and specialized user training testing. However, the Department's Talent Management System (TMS) and Security Touch Learning Management System retain training completion data, in which reports can be generated upon request. Procedures that define how documentation will be retained will be fully defined and implemented by December 30, 2011.

OIG Recommendation 13.2 Enhance the ISSO tracking tool to include contractor personnel and to store the proof of completion for all years.

Management Response: OCIO partially concurs with this recommendation. OCIO IAS will issue a memorandum to the Department's Principal Offices (POs) requiring contractors to take annual awareness training using the public facing Security Touch learning management web application for the FY12 training cycle. Security Touch will allow OCIO IAS to track and store proof of completion for all users. In instances where vendors use their own IT security training program or products to train their employees, OCIO will accept a certification letter from the company's authorized official that contains the listing of employees who completed the training along with a description of the training provided.

Plan of Action and Milestones Process Was Not Adequately Managed

OIG Recommendation 14.1 Develop procedures to ensure that the Plans of Action and Milestones (POA&M) program is maintained that it always reflects the current status of open and closed POA&Ms.

Management Response: OCIO concurs with this recommendation. OCIO will fully utilize the Department's POA&M repository, OVMS, to maintain the current status of open and closed POA&Ms. OCIO currently produces a weekly spotlight chart that contains all open POA&M items which are sent to each Principal Office that has any open POA&M on a bi-weekly basis. These reports will continue to be generated from OVMS to ensure the status being reported is accurate and up to date. The 30-60-90 day OVMS POA&M reports will be discussed quarterly at the ISSO meeting and metrics will be presented to the IA Board of Directors quarterly.

OIG Recommendation 14.2 Develop procedures to monitor the remediation of all actions within the POA&M population.

Management Response: OCIO concurs with this recommendation. OCIO IAS reviews POA&M status on a weekly basis and produces a weekly spotlight chart that contains all open POA&M items. The IV&V Team sends individual spotlight charts to each PO that has any open POA&M on a bi-weekly basis. The POA&M guide will be updated to include the process for sending spotlight charts and procedures for informing management when POA&M milestones are not met. This process will be fully implemented by December 31, 2011.

OIG Recommendation 14.3 Develop procedures to estimate and record the resource requirements for implementing proposed corrective action in accordance with OMB Exhibits 53 and 300.

Management Response: OCIO concurs with this recommendation. OCIO will use an existing data field in OVMS to ensure resources that are required by OMB A-11 Exhibit 300 and 53. OCIO will also ensure that all ISSOs are educated on how to properly enter resources required when remediating a POA&M. This process will be fully implemented by December 31, 2011.

OIG Recommendation 14.4 Develop an automated process to identify, track, maintain, and report security weaknesses resulting from the monthly vulnerability scans.

Management Response: OCIO concurs with this recommendation. OCIO IAS is currently working to implement an enhancement in OVMS which will allow for the automatic injection of FoundStone vulnerability scan files. This enhancement will automatically generate POA&Ms for each deficiency listed in a vulnerability report. This new system capability will allow OCIO to obtain an accurate inventory of the number of security control risks identified from monthly vulnerability scans. This enhancement is scheduled to be completed by March 31, 2012.

OCIO IAS is currently working on upgrades to OVMS as well as implementing a CM system which will track, maintain, and report security weaknesses. At Full Operational Capability it will also assign responsibility and tasking to the responsible party.

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) 345-6253 or Danny.Harris@ed.gov.