

# **REPORT OF THE INDEPENDENT AUDITORS**

## **Education Central Automated Processing System (EDCAPS) Information Security Audit**



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

**September 7, 2012**





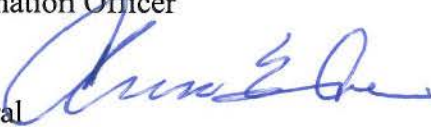
**UNITED STATES DEPARTMENT OF EDUCATION**  
OFFICE OF INSPECTOR GENERAL

Information Technology Audit Division

September 7, 2012

**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 Crime Investigations

SUBJECT: Final Report of the Independent Auditors  
Education Central Automated Processing System (EDCAPS) Information  
Security Audit ED-OIG/A11M0002

Attached is the Education Central Automated Processing System information security **final audit report**. We contracted with the independent certified public accounting firm of Williams, Adley & Company-DC, LLC (Williams Adley) to conduct this audit. The objective of the audit was to determine whether information technology security controls and effective management controls are in place to protect Departmental resources, including safeguarding personally identifiable information in accordance with the Federal Information Security Management Act and the Office of Management and Budget and National Institute of Standards and Technology regulation and standards. The audit assessed the information and information system security controls in place from October 1, 2011, through March 30, 2012.

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 of the draft report was provided to your Audit Liaison Officer. The Chief Information Officer's (OCIO) management comments and the corrective action plan for each of the recommendations contained in the draft report were evaluated. Appendix C of this report contains the OCIO's management responses to each of the findings. Recommendations were modified where appropriate to address management's comments.

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

In accordance with the Inspector General Act of 1978, as amended, the OIG 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), this report is 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.

We appreciate the cooperation shown to Williams Adley and the OIG during this audit. Should you or your office have any questions, please contact Joseph Maranto at (202) 245-7044, or [joseph.maranto@ed.gov](mailto:joseph.maranto@ed.gov).

Enclosure

cc: Steve Grewal, Acting Director, Information Assurance Services, 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, Audit Accountability and Resolution Tracking System Administrator, Office of Inspector General





September 7, 2012

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

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

U.S. Department of Education  
Office of Inspector General  
550 12th Street, S.W.  
Washington, DC 20202

**RE: Final Report of the Education Central Automated Processing System Security Controls Review**

Williams, Adley & Company-DC, LLP (referred to as “we” in this letter), is pleased to provide the Office of Inspector General (OIG) the final results of our review and independent assessment of the U.S. Department of Education (Department) information system security controls over the Education Central Automated Processing System (EDCAPS). Our audit objective was to determine whether information technology security controls and effective management controls are in place to protect Departmental resources, including the safeguarding of personally identifiable information. The scope of the audit was to determine whether the Department has developed and implemented adequate information system security controls to properly secure and safeguard EDCAPS and the Department’s data in accordance with the Federal Information Security Management Act, the Office of Management and Budget, and National Institute of Standards and Technology regulations and standards. We assessed the information system security controls in place from October 1, 2011, through March 30, 2012.

This review, performed under Contract No. ED-08-DO-0046, Task Order 2, was designed to meet the objectives identified in Appendix A, “Objectives, Scope, and Methodology,” of the report. We conducted this performance audit in accordance with Government Auditing Standards.

Should you have any questions, please contact Ben Nakhavanit or Robert Fulkerson at (202) 371-1397.

Sincerely,

A handwritten signature in black ink, appearing to read 'K. Isiaq', written over a light blue horizontal line.

Kola A. Isiaq, CPA, CISA  
Managing Partner

## Table of Contents

Acronyms, Abbreviations, and Short Forms Used in This Report .....	i
<b>I. Executive Summary .....</b>	<b>1</b>
<b>II. Background .....</b>	<b>3</b>
<b>III. Results of Review.....</b>	<b>6</b>
1. The Risk Management Framework Needs Improvement .....	7
2. Patch Management Needed Improvement .....	9
3. EDCAPS Security Configuration Management Controls Needed Improvement .....	12
4. Keylogger Incident Reporting for G5 Needs Improvement.....	16
5. Configuration Management Database Is Not Properly Maintained .....	17
6. The Department Has Not Implemented a Security Configuration Baseline .....	18
7. Separation of Duties Needed for G5 Application Users .....	20
<b>Appendix A: Objectives, Scope, and Methodology.....</b>	<b>22</b>
<b>Appendix B: EDCAPS System Description.....</b>	<b>25</b>
<b>Appendix C: Office of Chief Information Officer Comments .....</b>	<b>27</b>

## Acronyms, Abbreviations, and Short Forms Used in This Report

<b>ATO</b>	Authorization to Operate
<b>CPSS</b>	Contracts and Purchasing Support Software
<b>Dell</b>	Dell Services Federal Government
<b>Department</b>	U.S. Department of Education
<b>DUNS</b>	Data Universal Numbering System
<b>EDCAPS</b>	Education Central Automated Processing System
<b>EDCIRC</b>	Education Computer Incident Response Capability
<b>EDUCATE</b>	Education Department Utility for Communications, Applications, and Technology Environment
<b>FISMA</b>	Federal Information Security Management Act
<b>FMSS</b>	Financial Management System Software
<b>FSA</b>	Federal Student Aid
<b>FSS</b>	Financial System Services
<b>G5</b>	Grants Management System
<b>GAGAS</b>	Generally Accepted Government Auditing Standards
<b>NIST</b>	National Institute of Standards and Technology
<b>OCIO</b>	Office of the Chief Information Officer
<b>OIG</b>	Office of Inspector General
<b>OMB</b>	Office of Management and Budget
<b>OVMS</b>	Operational Vulnerability Management System
<b>SLA</b>	Service Level Agreement
<b>SP</b>	Special Publications
<b>US-CERT</b>	U.S. Computer Emergency Response Team

## I. Executive Summary

The audit assessed the effectiveness of the U.S. Department of Education's (Department) overall information security program and practices for the Education Central Automated Processing System (EDCAPS) in accordance with the E-Government Act (Public Law 107-347), including Title III, the Federal Information Security Management Act of 2002 (FISMA), the Office of Management and Budget (OMB), and National Institute of Standards and Technology (NIST) standards and guidance. The audit team concluded that the Department's information systems security program controls over EDCAPS need improvement to address the operational, managerial, and technical security control weaknesses identified in this report. The following control areas need improvement:

1. Risk Management
2. Patch Management
3. Security Configuration Management
4. Incident Reporting
5. Configuration Management Database Tracking
6. Security Configuration Baseline
7. Separation of Duties for G5 Users

Based on Williams Adley's review, the causes of the security control weaknesses generally fall into the following areas:

1. Office of the Chief Information Officer (OCIO) monitoring and oversight controls are not sufficiently designed or implemented to ensure contractor compliance with Federal requirements.
2. The OCIO internal control procedures are not sufficient to ensure that system owners and other responsible parties timely perform their assigned duties.

Many of the specific system security conditions contained in this report are similar in nature to the conditions previously identified in the audit report entitled "Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) Information Security Audit," ED-OIG/A11L0001, September 2011. Additionally, two of the findings are repeat conditions that have been identified every year since 2008. These conditions are identified in this report as repeat or modified repeat conditions.

This report contains specific recommendations that require the OCIO to strengthen existing controls and develop new monitoring capabilities designed to ensure OCIO and its contractors comply with Federal information system security laws, regulations, and standards. Additionally, the recommendations will provide an adequate level of auditability and help ensure sensitive and financial data that the system processed and maintained are properly secured and safeguarded from unauthorized access, data misuse, and fraudulent activities.

The audit was limited to a review and test of the information security controls covering EDCAPS, which is a major application that resides on the EDUCATE network. EDCAPS



consists of the Financial Management System Software, Contracts and Purchasing Support Software and the Grants Management System. In addition, Williams Adley conducted network scans and vulnerabilities tests of the wide-area and local-area network hardware consisting of network servers, routers, switches, and external firewalls that support EDCAPS. Vulnerability tests also covered the network gateways to the Internet.

Williams Adley assessed and tested the information security controls in place at the Department's Washington, D.C., headquarters, and at the service provider's data processing facility in Plano, Texas. The audit covered October 1, 2011, through March 30, 2012.

Based on our audit tests, nothing came to our attention for the following control areas:

- EDCAPS User Account Management
- Contingency Planning for EDCAPS
- EDCAPS Security Awareness Training

OCIO concurred with 9 of the 17 recommendations (1.3, 2.1, 2.2, 2.3, 4.1, 5.3, 6.2, 6.3, and 7.1), partially concurred with 7 of the 17 recommendations (1.1, 1.2, 3.1, 3.2, 5.1, 5.2, and 6.1), and did not concur with 1 recommendation (7.2) contained in the draft report issued to OCIO on July 6, 2012. Based on management comments, we modified some recommendations and deleted Recommendation 7.2 from the draft report.

We evaluated OCIO's comments related to the recommendations and the corrective actions OCIO has taken since March 2012 or has proposed to take to address the control weaknesses. However, the audit team did not verify whether the corrective actions OCIO has taken resolved the cited deficiencies.

## II. Background

The audit was limited to an assessment of the effectiveness of the Department of Education's (Department) overall information security program and practices for the Education Central Automated Processing System (EDCAPS) in accordance with the E-Government Act (Public Law 107-347), including Title III, the Federal Information Security Management Act of 2002 (FISMA), the Office of Management and Budget (OMB), and National Institute of Standards and Technology (NIST) standards and guidance.

The audit included, but was not limited to:

- Assessing the Department's and EDCAPS' policies, procedures, and controls against
  - NIST Federal Information Processing Standard Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006;
  - NIST Special Publication (SP) 800-37, Revision 1, "Guide For Applying The Risk Management Framework To Federal Information Systems," February 2010;
  - NIST SP 800-39, "Managing Information Security Risk," March 2011;
  - NIST SP 800-61, Revision 1, "Computer Security Incident Handling Guide," March 2008;
  - NIST SP 800-52, "Guidelines for the Selection and Use of Transport Layer Security (TLS) and Implementations," June 2005;
  - NIST SP 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," August 2009;
  - NIST SP 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems," February 2006; and
  - NIST SP 800-70, Revision 2, "National Checklist Program for IT Products – Guidelines for Checklist Users and Developers," February 2011.
- Assessing the effectiveness of the Department's management oversight controls as required by OMB Circular A-130 Appendix 3, "Security of Federal Automated Information Resources," NIST Federal Information Processing Standard Publication 140-2, and FISMA.
- Testing select general and application controls and key management oversight controls, agreed on by the Office of Inspector General (OIG).
- Performing security reviews of designated information systems and applications by conducting vulnerability assessments and penetration testing of EDCAPS. The tests determined the adequacy of the Department's network security controls to prevent or detect unauthorized activities from internal hackers and threats. The tests also determined the adequacy of the controls to identify and prevent viruses and other advanced persistent threats from entering the network and Department hardware.

## EDCAPS Operating Structure

The Department entered into a contract with a third party information technology service provider, Dell Services Federal Government (Dell),<sup>1</sup> whereby the Department obtains all information technology services from the Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) contractor. Under this contractor-owned and contractor-operated contract, the contractor owns the Department's information technology infrastructure (hardware, communication devices, and operating systems) and provides all human resources to operate, support, and maintain the information technology infrastructure all day, every day. The Office of the Chief Information Officer (OCIO) monitors and oversees the contractor's performance, including ensuring that the contractor's information system security controls meet or exceed the Department's requirements and Federal laws, regulations, and standards. The OCIO monitors and evaluates the contractor-provided information technology services through a service level agreement (SLA) framework.

The OCIO has categorized EDCAPS as a moderate impact major application that is critical to the business processes and mission of the Department. EDCAPS is a suite of financial applications (subsystems) including commercial off-the-shelf and custom code and interfaces that encompass the Department's core financial management processes. EDCAPS provides the following functions:

- General ledger—Preparation of financial statements and reconciliation of general ledger balances with subsystems maintained in program areas and with Treasury
- Funds management—Budget formulation, budget execution, and funds control
- Grants—Processing before and after grants are awarded, including grant payment processing
- Contract—Processing before and after contracts are awarded
- Receivables management
- Cost management
- Recipient management
- Administrative processes

EDCAPS consists of the following subsystems:

- Financial Management System Software (FMSS)
- Contracts and Purchasing Support Software (CPSS)<sup>2</sup>
- Grants Management System (G5)<sup>3</sup>

---

<sup>1</sup> Perot Systems, the contract holder, was acquired by Dell Services Federal Government in September 2009.

<sup>2</sup> CPSS and FMSS subsystems do not collect personally identifiable information.

<sup>3</sup> The G5 application collects the names, addresses, telephone numbers, Social Security numbers, e-mail addresses, and bank account numbers of individuals and vendors receiving fellowship grants. The application component e-Grants of G5 collects names, addresses, telephone numbers, and e-mail addresses for user registration purposes.

Although the OCIO is responsible for ensuring that adequate information system and security controls within the Department have been designed, implemented, and maintained, the OCIO has delegated various EDCAPS system responsibilities to the following individuals:

- The Chief Financial Officer is the owner of all information that is processed, stored, and transmitted by EDCAPS.
- The Director of the Financial Systems Services (FSS), which is part of the OCIO, is the system owner and is responsible for maintaining the system and complying with appropriate Federal laws, regulations, and standards and information security measures.
- The Manager of the Systems Operations and Maintenance Team, which is part of the OCIO, is responsible for daily systems operations.
- The EDCAPS Information System Security Officer, which is part of the OCIO, is responsible for the security of EDCAPS.

Information Assurance Services, which is part of the OCIO, conducts the security authorization testing for EDCAPS systems.

The majority of EDCAPS hardware is physically located at the Dell data processing facility in Plano, Texas. The EDCAPS System Security Plan states that EDCAPS serves about 2,500 internal users at the Department's headquarters and 21,000 external users across the nation and worldwide. The external users have access to the Web-based application, G5. Internal users must have an EDUCATE user account and an EDCAPS application user account to access EDCAPS applications.

The EDUCATE service provider, Dell, manages Windows User accounts through the EDUCATE administrators. EDCAPS administrators handle application accounts. EDUCATE provides security services to EDCAPS that include:

- monitoring and maintaining log files for AIX (UNIX),
- alerting EDCAPS of security breaches,
- providing help desk services, and
- providing network support services.

### III. Results of Review

The audit team concluded that the Department's information and information systems security program controls over EDCAPS need improvement to address the operational, managerial, and technical security control weaknesses identified in this report. The security control weaknesses fall into the following areas.

1. Risk management framework is not sufficiently designed or implemented to address risk from an organizational perspective and reflect change within the system in a timely manner.
2. Monitoring and oversight controls were not sufficiently implemented to address patch management control deficiencies.
3. Security controls weaknesses existed for hardware and software configurations.
4. Monitoring controls are not sufficiently designed to ensure that correct actions for incidents are taken in a timely manner and properly documented.
5. Configuration Management Database was not adequately maintained and updated to track EDCAPS hardware changes.
6. Security configuration baselines have not been established for operating systems, databases, and network infrastructure devices used for EDCAPS.
7. Business application control procedures are not sufficient to ensure ongoing monitoring of information system connection.

Many of the conditions of system security weaknesses contained in this report are similar in nature to the conditions previously identified in last year's OIG EDUCATE and FISMA audit reports.<sup>4</sup> Additionally, the same conditions were identified in two other relevant OIG information technology security reports.<sup>5</sup>

The audit team assessed and tested the information security controls in place at the data center located in Plano, Texas and at the Department's OCIO and other program offices from October 1, 2011, through March 30, 2012.

Based on our audit tests, nothing came to our attention for the following control areas:

- EDCAPS User Account Management
- Contingency Planning for EDCAPS
- Security Awareness Training

Below are the audit results in order of highest to lowest risk.

---

<sup>4</sup> "Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) Information Security Audit," [ED-OIG/A11L0001](#), September 2011; "U.S. Department of Education's Compliance with the Federal Information Security Management Act for Fiscal Year 2011," [ED-OIG/A11L0003](#), October 2011.

<sup>5</sup> "Incident Handling and Privacy Act Controls over External Web Sites," [ED-OIG/A11I0006](#), June 2009; "IT Security Controls over the Debt Management Collection Process, Phase II, Fiscal Year 2008," [ED-OIG/A11I0003](#); September 2008.

## 1. The Risk Management Framework Needs Improvement

The risk management framework was not sufficiently designed or implemented to ensure that system changes were reflected in a timely manner. Specifically, FSS did not perform and document the required EDCAPS and G5 security assessment in accordance with NIST and Departmental guidance.<sup>6</sup> Additionally, FSS did not have a formally approved risk assessment document to support that they performed a risk assessment before migrating Phase 3 of G5 into production. The self-assessment report provided by FSS did not include an authorized signature and date evidencing that the report was an official document and when it became operative. Further, FSS did not ensure the Authorization to Operate (ATO) letter was reauthorized after FSS implemented G5 Phase 3. The current ATO is dated September 30, 2009, and FSS installed the G5 Phase 3 into production in March 2011.

Based on document review and discussions with OCIO officials, we determined that the FSS team did not believe that the changes to G5 required the team to reassess the risks or that the changes required a new ATO.

NIST SP 800-53, Revision 3, requires agencies to update system risk assessments whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities) or other conditions that may impact the security state of the system or at least every 3 years to support the ATO. The OCIO has defined a “significant change” in OCIO-06-15 Handbook as a change that alters the mission, operating environment, basic vulnerabilities, or the security posture of the system. This includes changes of operational environment or contractor responsible for the application and maintenance of the system. Phase 3 represented a significant change as it replaced the GAPS and e-Grants applications, installed software, and converted data.

NIST SP 800-37, Revision 1, states that when an organization has a proposed or actual change to its information system or system’s operation environment, an organization must conduct a security impact analysis to determine the extent to which the changes affect the security state of the system. If the results of the security impact analysis indicate that the changes can affect or have affected the security state of the system, then corrective actions are initiated and security documents are revised and updated (that is, the security plan, security assessment report, and plan of action and milestones). The authorization official then determines whether a formal security reauthorization is needed.

By not performing a new risk assessment for the significant changes to the EDCAPS environment, the system owner and OCIO increase the security risks to EDCAPS for vulnerabilities to be exploited. Additionally, without updating the system risk assessment to

---

<sup>6</sup> NIST SP 800-37, Revision 1, “Guide for Applying the Risk Management Framework to Federal Information Systems,” February 2010; NIST SP 800-39, “Managing Information Security Risk,” March 2011; NIST SP 800-53, “Recommended Security Controls for Federal Information Systems and Organizations,” Revision 3, August 2009 with updates as of May 2010; and OCIO-06-15 Handbook, “Security Authorization Guidance,” June 2011.



identify and document security weaknesses, the system owner responsible will not be made properly aware of significant security concerns to initiate corrective action in a timely manner.

We noted that as of April 2012, Information Assurance Services is conducting the security assessment and risk analysis and tests required for the security authorization process on the G5 system to support a revised ATO.

## **RECOMMENDATIONS**

- 1.1 We recommend that OCIO improve the risk management framework by creating a review process where the implementation of a new system or the change to an existing system requires concurrence by upper management with the systems owner's risk assessment.

We recommend that the OCIO direct the FSS system owner to:

- 1.2 Perform and document a risk assessment for G5 Phase 3 and update, approve, and date the necessary documents.
- 1.3 Complete the security authorization process and submit an updated ATO letter for G5 Phase 3.

## **Management Response**

OCIO partially concurred with Recommendations 1.1 and 1.2. For Recommendation 1.1, OCIO stated that the review process already exists where the implementation of a new system, or a change to an existing system, requires review and approval by levels of management based on the results of a risk assessment. Although the review process exists, OCIO recognizes it can improve the execution of the risk management framework. OCIO has requested additional funding in fiscal year 2014 to make the Department's risk management framework more robust and proactive in terms of detailed reviews, quality, and effectiveness.

For Recommendation 1.2, OCIO stated that before EDCAPS G5, Phase 2 became operational, OCIO performed and completed the required certification and accreditation of the system and granted an ATO for G5 Phase 2. Since the G5 Phase 3 release included changes to only the business functionality and not the IT infrastructure, Information Assurance Services determined (and noted in the proceedings of the Enterprise Architecture Review Board) that new risk assessment documents were not required at that time. Also, to maintain the existing EDCAPS ATO, the annual security assessment for EDCAPS, which includes G5, will be completed by September 30, 2012.

OCIO concurred with Recommendation 1.3.

## **OIG Response**

We reviewed management's response and look forward to OCIO improving the execution of the Department's risk management framework for Recommendation 1.1, including performing the annual security assessment for EDCAPS by September 30, 2012.

For Recommendation 1.2, we requested but did not receive any evidence from the Information Assurance Services or Enterprise Architecture Review Board noting that new risk assessments for EDCAPS G5 were not required. We were also not provided any evidence of a formally approved risk assessment document. Therefore, the Department should perform and document a risk assessment for G5 Phase 3 and update, approve, and date the necessary documents.

## **2. Patch Management Needed Improvement**

Based on our EDCAPS network scans and testing results, we determined that OCIO has not implemented sufficient monitoring and oversight controls enterprise-wide to ensure recommendations from prior OIG reports were implemented to address the patch management control deficiencies. The audit team provided the OCIO the detailed information on the results of all of the scans and testing it completed, as well as vulnerabilities for remediation.

Five previous OIG audit reports, dated from September 2008 through October 2011, identified these potential network vulnerabilities and the patch management control deficiencies. In a 2008 report, the OIG reported that Federal Student Aid (FSA) needed to improve controls over risk assessment for the Debt Management Collection System and use scanning tools and techniques to identify and correct vulnerabilities, including needed patches (Finding No. 2).<sup>7</sup> In a June 2009 report, the OIG reported that the OCIO and the contractor did not protect all Web sites by timely implementing updates and system patches (Finding No. 3).<sup>8</sup> In September 2010, the OIG found that FSA did not ensure that the contractor performed adequate and timely patch management.<sup>9</sup> In September 2011, the OIG found that the OCIO had not defined timeframes for installing security patches on network devices in the SLA with Dell and that critical security patches were not installed.<sup>10</sup> In October 2011, the OIG reported that the OCIO still had not established and implemented formal, enterprise-wide patch management policies and procedures consistent with NIST requirements.<sup>11</sup> All five reports identified conditions that existed at the EDUCATE and OCIO program level. Therefore, this is a modified repeat condition.

---

<sup>7</sup> "IT Security Controls over the Debt Management Collection Process, Phase II, Fiscal Year 2008," ED-OIG/A11I0003, September 30, 2008.

<sup>8</sup> "Incident Handling and Privacy Act Controls over External Web Sites," [ED-OIG/A11I0006](#), June 10, 2009.

<sup>9</sup> "Security Controls for Data Protection over the Virtual Data Center," ED-OIG/A11J0006, September 29, 2010.

<sup>10</sup> "Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) Information Security Audit," [ED-OIG/A11L0001](#), September 2011.

<sup>11</sup> "The U.S. Department of Education's Compliance with the Federal Information Security Management Act for Fiscal Year 2011," [ED-OIG/A11L0003](#), October 2011.

The audit team found the following patch management weaknesses while performing vulnerability scanning and testing.

A. Use of software that is no longer supported by vendors or not installing current patches.

- The Technology Levels (that is, versions) of 16 production AIX (UNIX) systems were not up to date. These systems are missing critical security patches.
- Six production UNIX systems are running versions of IBM WebSphere Application server that are multiple versions behind the current release, making the systems vulnerable to multiple application-level attacks. The fix pack installed is number 33 (release February 13, 2009), instead of the current fix pack 43 (released September 27, 2010).
- Three G5 production Apache Web servers are vulnerable to denial-of-service attacks and another G5 production server is vulnerable to buffer overflow attacks. The Apache Web servers do not have the latest patches.
- The Cognos Web application has an unsupported version of Internet Information Services Web server, Adobe Reader, and Microsoft Office. These unsupported versions make the system vulnerable to attacks.
- One server is running the Windows 2000 operating system, which Microsoft no longer supports. Microsoft will not release security patches and other software fixes for Windows 2000, making this server more vulnerable to attacks.

B. G5 database vulnerabilities.

- Three critical vendor security patches (released by the vendor more than 3 months from the time of testing) for two Oracle databases have not been installed, making them susceptible to cyber attacks. The security patches condition was previously identified during the fiscal year 2011 EDUCATE and FISMA audits.
- One Oracle database is missing critical patch updates dating back to April 2011, and another Oracle database is missing the most recent patchset.<sup>12</sup> This is a modified repeat condition, similar to the security patch weaknesses identified in the fiscal year 2011 OIG audit reports for EDUCATE and FISMA.
- Two Oracle databases have the remote login password file enabled, which does not provide a lockout feature and is potentially vulnerable to password attacks.
- Two Oracle databases give the PUBLIC role EXECUTE privilege on the SYS.UTL\_FILE, which potentially allows Procedural Language/Structured Query Language<sup>13</sup> to read from and write to files on the operating system.

---

<sup>12</sup> As of September 2012, the latest patchsets for Oracle were Oracle 9.2.0.8 on all platforms; Oracle 10.1.0.5 on all platforms; Oracle 10.2.0.5 on Linux x86, Linux x86-64, Windows x86-64; Oracle 10.2.0.3 on IBM z/OS; Oracle 10.2.0.4 on all other platforms; Oracle 11.1.0.7 on all platforms; and Oracle 11.2.0.2 on all platforms.

<sup>13</sup> Procedural Language/Structured Query Language is stored and compiled in Oracle Database and runs within the Oracle executable. It automatically inherits the robustness, security, and portability of Oracle Database.

NIST SP 800-53, Revision 3, requires the organization to identify, report, and correct information system flaws; test software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and incorporate flaw remediation into the organizational configuration management process. Additionally, the Department's contract with Dell requires Dell to install the most current security patches as soon as the patches are available from the vendor and are properly and successfully tested, as well as to install, maintain, and update standard hardware and software configurations. Further, the contract requires Dell to produce and submit deployment reports monthly to include, at a minimum, success and failure statistics of scheduled distributions such as patches or upgrades.

The OCIO did not adequately monitor or establish sufficient reporting requirements to ensure Dell Services Federal Government updated the systems with vendor-supplied security patches and to measure Dell's progress on remediating known vulnerabilities. Additionally, despite the OIG reporting these same conditions from 2008 through 2012, OCIO has not implemented a proactive enterprise-wide solution to patch all Department systems. If Dell does not carry out the functions that the SLA requires, OCIO may use the disincentive provisions in the SLA to lower Dell compensation, thereby encouraging better performance.

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

## RECOMMENDATIONS

We recommend that OCIO:

- 2.1 Require Dell and other contractors to comply with already agreed-on SLA requirements to install the security patches as soon as the patches are available from the vendor and after the patches have been properly tested to ensure patches do not adversely affect the system. The timeframe for testing and implementing patches should not exceed the required timeframes noted in the OCIO-01 Handbook.<sup>14</sup>

---

<sup>14</sup> As defined in the OCIO-01 Handbook, "Handbook for Information Security Assurance Policy," October 19, 2011, the timeframe in which an organization must acquire, test, and deploy (assuming the results of testing are satisfactory) a security patch depends on the risk level of the patch. Specifically, the timeframes are as follows: 72 hours for critical security patches, 7 days for high-risk security patches, 21 days for medium-risk security patches, and 30 days for low-risk security patches.

2.2 Enforce the disincentive contract clauses for Dell and other contractors for not meeting the provision in the SLA to timely implement patches.

2.3 Immediately correct or mitigate the vulnerabilities identified.

### **Management Response**

OCIO concurred with Recommendations 2.1, 2.2, and 2.3.

### **3. EDCAPS Security Configuration Management Controls Needed Improvement**

The audit team tested the EDCAPS hardware and software configurations against the Department of Defense “Security Technical Implementation Guides” recommended security controls.<sup>15</sup> The tests covered the EDCAPS servers and databases and G5 Web servers. In a 2011 report, the OIG reported that vulnerabilities in security configuration continued to exist (Finding No. 1).<sup>16</sup> Therefore, this is a modified repeat condition.

The audit team found the following configuration management weaknesses while performing external vulnerability scanning and testing.

- Secure Sockets Layer cookies are not used for multiple Web pages on the G5 application. The “secure” flag must be set for all user cookies. Failure to use the “secure” flag enables an attacker to access the session cookie by tricking the user’s browser into submitting a request to an unencrypted page on the site.
- G5 returns information in the Uniform Resource Locator<sup>17</sup> field that an unauthorized individual can potentially use to gain access to valid user accounts. Sensitive data must not be transmitted via Uniform Resource Locator arguments. Sensitive data should instead be stored in a server-side repository or within the user’s session.
- G5 allows simultaneous session logons for nonprivileged user accounts. When a user clicks on the browser back button to a previous page and then tries to go back to G5, a Tivoli splash page appears instead of the main page. A secure application must not give out unnecessary information such as the applications running on it because it allows an attacker access to more information.

Internal vulnerability scanning and testing identified the following vulnerabilities.

- Weak or default credentials are used to access system resources.

---

<sup>15</sup> NIST makes available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications. For specific systems, NIST refers to Department of Defense, Defense Information System Agency Security Technical Implementation Guides for guidance.

<sup>16</sup> “Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) Information Security Audit,” [ED-OIG/A11L0001](#), September 2011.

<sup>17</sup> A protocol for specifying addresses on the Internet.

- Netbios and Server Message Block network protocols share default or null passwords. This potentially allows users to establish unauthorized connections to network resources and obtain sensitive network information.
- Five systems have default community names enabled for the remote Simple Network Management Protocol service. An attacker may use this information to gain more knowledge about the remote host or to change the configuration of the remote system (if the default community privilege allows such modifications).
- A production system running Oracle GlassFish Server administration console has potential of authentication bypass vulnerability. The server fails to enforce authentication on hypertext transfer protocol requests that contain lower case method names (for example, “get”).
- The Sun ONE server console is using default login credentials. The default login may allow a local or remote user to gain unauthorized administrative access to the server.

The audit team found the following system misconfigurations within the EDCAPS environment.

- Eight production Windows servers have a service configured with privilege escalation vulnerability. This potentially allows a standard user account to exploit this vulnerability to execute arbitrary commands as a system account.
- A tape management system is running a network service, VxWorks WDB Debug Agent, which is vulnerable to an attacker executing arbitrary code on the system. Using this service, it is possible to execute arbitrary code on the host to enable the attacker to take complete control of the affected device.
- Password expiration for the G5 Web server was set to 0 (unlimited) for selected service accounts. This setting is not compliant with the G5 Security Configuration Checklist, which states “Password Expiration 90 days.” This condition exposes these accounts to unlimited and continuous attacks from malicious users.
- Three compiler programs<sup>18</sup> are installed on the G5 Web server, which exposes the server to unauthorized software changes and the installation of Trojan horses or viruses. For example, the attacker’s code can be uploaded and compiled to the Web server.
- The G5 Web server was running “sendmail” and “e-mail” services, thus exposing the server to unauthorized access through the e-mail protocols. Additionally, the e-mail application is a specialized application that requires the dedication of unnecessary server resources. DoD Web Server Security Technical Implementation Guides, Version 7, Release 1, September 2010, recommends that a production Web server should provide only hosting services for Web sites to reduce the risk of abuse as an e-mail relay.
- Antivirus software is not installed on one Web server.
- The Web server cryptographic protocol, Secure Sockets Layer Version 3, is not compliant with NIST SP 800-52, “Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations,” June 2005. NIST recommends enabling Transport Layer Security, Version 1.0 or greater, and disabling the Secure Sockets Layer.

---

<sup>18</sup> A compiler program translates source code into object code. The compiler derives its name from the way it works, looking at the entire piece of source code and collecting and reorganizing the instructions.



Examples of vulnerabilities found on the three EDCAPS AIX servers tested include the following.

- One non-super user account on a server does not have a password.
- Two servers are not configured with a logon banner.
- One server has passwords for five accounts set “not to expire.”
- Three servers have active accounts that no one has ever logged onto.
- Three servers have not disabled the “root” login by configuring the secure shell program to disable root login.
- Three servers have uneven file permission. That is, the file owner has fewer privileges than the group or world users and the file is owned by a privileged user or group (such as root or bin). Additionally, not all the run control scripts are owned by system accounts.

Examples of vulnerabilities found on the EDCAPS Windows servers include the following.

- Nine servers are configured to enumerate the user accounts and network shares. This allows anonymous logon users (null session connections) to list all account names and enumerate all shared resources, thus providing a map for system attacks.
- Eight servers directly log onto the system with administrator privileges when rebooted. This enables full access to any system utility during a system reboot.
- Nine servers are configured to use a weak authentication protocol “LanMan,” which is susceptible to password attacks, instead of Kerberos, a stronger authentication protocol.
- Nine servers allowed “anonymous” access to their network shares, where any shares listed can be accessed by any network user. This could lead to the exposure or corruption of sensitive data.
- Five servers are configured to save password changes in the Security Accounts Manager database using a weak encryption algorithm “Local Area Network Manager hash” to enable easy retrieval of users’ account passwords.
- Eight servers allow the Administrators group to debug programs to the kernel<sup>19</sup> with complete access to sensitive and critical operating system components.

The types and nature of the security risks identified indicate poor security configuration management practices that require immediate improvement. Additionally, the OIG previously identified these security risks in the fiscal year 2011 EDUCATE audit report. That they continue to exist indicates that OCIO has not made configuration management a priority. During the audit, the audit team provided the test result data to OCIO for immediate evaluation and remediation.

NIST SP 800-53, Revision 3, requires the organization to identify, report, and correct information system flaws and incorporate flaw remediation into the organizational configuration

---

<sup>19</sup> The kernel is a program that constitutes the central core of a computer operating system. It has complete control over everything that occurs in the system.

management process. Additionally, agencies are required to develop and implement mandatory configuration settings<sup>20</sup> and ensure compliance with them.

The OCIO did not implement remedial actions to address previously identified security weaknesses and did not establish a proactive enterprise-wide process to fix the vulnerabilities identified during previous audits.

## **RECOMMENDATIONS**

We recommend that OCIO:

- 3.1 Implement an enterprise approach with established implementation dates to enforce mandatory security configuration settings for the EDCAPS system and all other Department systems. OCIO and Dell should document all agreed-on implementation dates for fixing all enterprise-wide patching and configuration vulnerabilities.
- 3.2 Establish reporting procedures to monitor Dell's monthly progress to ensure identified vulnerabilities are fixed within the established timelines.

### **Management Response**

OCIO partially concurred with Recommendations 3.1 and 3.2. For Recommendation 3.1, with respect to an enterprise approach to enforce mandatory security configuration settings, OCIO has published "Information Technology Security Configuration Management Guidance," February 20, 2009, which states, "All ED information system owners will ensure their systems undergo a baseline security configuration validation on an annual basis" and provides guidelines for ensuring compliance. This guidance and the Department's security authorization and Plan of Action and Milestones processes comprise OCIO's enterprise approach to enforcing mandatory security configuration settings. While an enterprise approach exists, OCIO recognizes that it can improve the execution of the Department's configuration management control. OCIO Information Technology Services and FSS will work with the appropriate vendors to document implementation dates for addressing all specific vulnerabilities identified within the audit report by September 30, 2012.

For Recommendation 3.2, OCIO Information Assurance Services already monitors the EDUCATE program's progress toward remediating identified vulnerabilities, as with all other programs, through the Operational Vulnerability Management System (OVMS) and the tracking of open Plan of Action and Milestones in accordance with the timelines established in the Department "Plan of Actions and Milestones Guidance." OCIO recognizes that it can improve the reporting and tracking of vulnerabilities and their remediation and will work with Dell to

---

<sup>20</sup> Configuration settings are the configurable security-related parameters of information products that are part of the information system. Security-related parameters include, for example, registry settings; account, file, and directory (that is, permissions) settings; and settings for network ports.

continually enhance the existing reporting and monitoring processes. OCIO stated that corrective action by a specific date is not applicable.

### **OIG Response**

We reviewed management's response and do not agree with OCIO's response for Recommendation 3.1. For Recommendation 3.1, we were not provided evidence of detailed documentation (for example, guidelines and procedures) for mandatory security configuration settings that would allow systems personnel to consistently configure their systems to support OCIO assertions. For Recommendation 3.2, although OCIO states it monitors the contractor's progress toward remediating identified vulnerabilities, we were not provided evidence that the monitoring has fixed the control weakness. As the finding states, in a 2011 report, the OIG reported that vulnerabilities in security configuration continued to exist and the same condition continues to exist. Although we recognize that OCIO has made efforts to resolve this situation, our test results clearly show that the current controls are not achieving the desired results and require OCIO to enhance its control process. We encourage OCIO to work with Dell to continually enhance the existing reporting and monitoring processes and fix the vulnerabilities in a timely manner.

## **4. Keylogger Incident Reporting for G5 Needs Improvement**

OCIO has not established and implemented effective controls to review, reconcile, track, report, and resolve the G5 keylogger incidents.<sup>21</sup> From our test of 4 keylogger incidents that the United States Computer Emergency Response Team (US-CERT) reported,<sup>22</sup> the audit team determined none were entered in OVMS as required to ensure compliance with NIST SP 800-53, Revision 3 guidance. The Education Computer Incident Response Capability team (EDCIRC) receives a weekly Keylogger Report from US-CERT and is responsible for entering the incident information into OVMS. OVMS then generates an automatic e-mail notice to the EDCIRC and the Privacy Advocate to document that an incident has been created in OVMS.

Additionally, the audit team found that the EDCIRC processes and controls for capturing incident information and entering the incident into OVMS are inadequate to ensure all incidents are entered into OVMS.

The audit team found that the EDCIRC had not established procedures to reconcile the incidents reported by the US-CERT with the incidents entered into OVMS so as to ensure that all G5 keylogger incidents are recorded. Additionally, the OCIO-14 Handbook<sup>23</sup> does not specifically address G5 keylogger incidents as a required event for recording into OVMS.

---

<sup>21</sup> Keylogging is a method of capturing and recording users' keystrokes.

<sup>22</sup> From October 11, 2011, through January 24, 2012, the US-CERT reported 44 G5 keyloggers. We selected 10 percent per our sampling methodology.

<sup>23</sup> OCIO-14 Handbook, "Handbook for Information Security Incident Response and Reporting Procedures," June 26, 2007.

NIST SP 800-53, Revision 3, requires an agency to track and document information system security incidents obtained from various sources such as US-CERT. Failure to update OVMS for incidents, like keylogging, that US-CERT reports increases the risk that system owners and data owners will not take appropriate action to timely resolve security exposures to prevent unauthorized access, release, and misuse of sensitive and personal information.

## **RECOMMENDATION**

- 4.1 We recommend that OCIO revise the OCIO-14 Handbook to require the EDCIRC to enter all keylogger incidents reported by US-CERT into OVMS and use OVMS to review, reconcile, track, report, and resolve the all keylogger incidents, not just G5.

### **Management Response**

OCIO concurred with the recommendation.

## **5. Configuration Management Database Is Not Properly Maintained**

The Configuration Management Database is not adequately maintained and updated to track hardware changes applicable to the current EDCAPS environment. The audit team found that Dell has not recorded in the Configuration Management Database two EDCAPS servers that OCIO is currently using.

Although Dell provides a General Event Notification Quarterly Configuration Management Report to OCIO of current hardware in use within the EDUCATE operating environment as a part of inventory tracking, OCIO does not oversee the process to ensure that Information Technology Services adequately reconcile the reports Dell issues.

NIST SP 800-53, Revision 3, requires an agency to develop, document, and maintain an inventory of information system components (hardware and software) that accurately reflects the current information system. Further, the current Performance Work Statement requires Dell to update, at least weekly, the Department's Asset Management System and reconcile it with Dell's inventory management system data at least once a month. To encourage Dell performance, OCIO built into the SLA a disincentive provision, such as reducing Dell's compensation, that penalizes Dell for nonperformance.

Without accurate accountability of all authorized and current servers connected to the network, OCIO increases the risk that unauthorized activities can occur and go undetected.

## RECOMMENDATIONS

We recommend that OCIO:

- 5.1 Enforce the Performance Work Statement requirement requiring Dell to implement procedures to update the Department's Asset Management System of Record and to reconcile it with Dell's inventory management system data at least once a month.
- 5.2 Require the Information Technology Services Group to perform a review and reconciliation of hardware to ensure the information Dell reports is accurate.

### **Management Response**

OCIO partially concurred with Recommendations 5.1 and 5.2 and indicated that currently, the EDUCATE contract has no SLA requirements for Dell to implement procedures to update the Department's Asset Management System or the Configuration Management Database. OCIO's Information Technology Services continues to work with Dell to improve procedures to update and reconcile the Department's assets. Corrective action by a specific date is not applicable.

OCIO concurred with Recommendation 5.3.

### **OIG Response**

We assessed the OCIO's response and modified the finding and recommendations. The body of the finding was revised and SLA was replaced with Performance Work Statement. We also modified Recommendation 5.1 to reflect constraints from the Performance Work Statement. In addition, we removed the former Recommendation 5.2 referring to enforcing SLA disincentives, and re-numbered the former Recommendation 5.3 to 5.2.

## 6. The Department Has Not Implemented a Security Configuration Baseline

EDCAPS is one of the business systems that is supported by EDUCATE.<sup>24</sup> EDUCATE configuration baseline documentation for Windows 2003, Windows 2008, UNIX and Oracle, are in draft status and pending Information System Security Officer approval, resulting in noncompliance with NIST SP 800-53, Revision 3. OCIO Information Assurance officials stated that the EDUCATE baseline was still pending Information System Security Officer approval and, therefore, it had not been implemented. According to the Information Assurance officials, the Security Architect and the Information System Security Manager must review and approve the draft configuration baseline for Windows 2003, Windows 2008, UNIX, and Oracle. The timeframe for the approval process is uncertain since the Information System Security Manager

---

<sup>24</sup> EDUCATE subsystems includes (1) the EDUCATION Network Infrastructure System, (2) the EDUCATE Mass Storage System, (3) the EDUCATE Security Operations Center, (4) EDCAPS, (5) the EDUCATE Data Center Information System, and (6) the Case Activity Management System.

position was vacant at the time of the audit. Once the Security Architect and the Information System Security Manager approve the configuration baselines, they will send the baselines to OCIO management, FSA, the Privacy Office, and the Office of General Counsel for their comments. Then the Information System Security Officer will sign the final baseline configuration document.

NIST SP 800-53, Revision 3, requires an agency to develop, document, and maintain under configuration control a current baseline configuration of the information system. Additionally, the OCIO-11, "Handbook for Information Technology Security Configuration Management Planning Procedures," requires the effective management of changes and a formal, documented, systematic process for requesting, evaluating, tracking, and approving changes to a general support system and major application.

Without a baseline configuration for EDUCATE, the Department may not be maintaining accurate information about the components of EDUCATE (for example, the standard software load for a workstation, server, network component, or mobile device including operating system and installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture.

## **RECOMMENDATIONS**

We recommend that OCIO:

- 6.1 Expedite the review and approval of the draft baseline configuration documents.
- 6.2 Provide an alternative or acting position for the System Security Manager's position to approve the draft baseline configuration documents and maintain up-to-date baseline configuration documentation with vendor and Department specifications and changes.
- 6.3 Establish procedures to effectively cross-train OCIO personnel in all critical positions and functions to ensure workload and processes are not compromised when vacancies occur.

## **Management Response**

OCIO partially concurred with Recommendation 6.1. OCIO Information Assurance Services published the "Information Technology Security Baseline Configuration Guidance" on February 20, 2009. This document requires system owners to ensure their systems undergo a baseline security configuration validation. This document also specifies that information technology system owners will ensure compliance with established baseline configuration standards of the NIST National Checklist Program. For information technology systems that have components (such as Mac and Linux) not addressed within the NIST National Checklist Program, a benchmark from the Center for Internet Security can be used. If an information technology system has components not addressed by either of the former configuration standards, component vendor security and/or industry best practice security configurations must be employed. OCIO recognizes it can improve the execution of the Department's security



configuration baseline controls establishment and oversight processes and will endeavor to make these enhancements. OCIO stated that corrective action by a specific date is not applicable.

OCIO concurred with Recommendations 6.2 and 6.3.

### **OIG Response**

We do not agree with management's response for Recommendation 6.1. Although OCIO is using a standard checklist to validate its system security configuration, the audit found that the checklist was not appropriately modified to consider the technical environment for the EDCAPS system and did not fully consider the unique operational requirements to ensure the checklist met the intent and purpose of the NIST National Checklist Program. NIST SP 800-70, Revision 2, requires that users should take their operational environments when selecting appropriate checklists, and users should customize and test checklists before applying them to production systems. The "Information Technology Security Baseline Configuration Guidance" does not give specific guidance to Department personnel on how to configure systems.

## **7. Separation of Duties Needed for G5 Application Users**

The EDCAPS system team notifies certain OIG and Department personnel of known improper payments. The audit team examined the cause of one such improper payment. This particular improper payment exposed sensitive grantee award information to a grantee because of an erroneous reassignment of a Data Universal Numbering System (DUNS) number. This error resulted in two grantees seeing each other's awards in the G5 system. The audit team conducted further research to determine the cause of the DUNS reassignment error and found FSA requested a G5 team member to enter a DUNS number in G5. However, the DUNS number that FSA requested was incorrect, resulting in the Department making a grant payment to an incorrect grantee.

The error occurred because the EDCAPS G5 team does not independently review the DUNS reassignments entered in the G5 system to verify that the DUNS numbers are correct and FSA approved them.

The DUNS number in G5 is prepopulated with the grantees' profile information such as grantee name and address as downloaded from the Central Contractor Registry<sup>25</sup> database. The DUNS numbers are accessible to the G5 team in the G5 system to enable further verification of grantees' profile changes, including DUNS reassignments. When a DUNS reassignment is performed, the DUNS number requested should match the grantee profile in the G5 system as downloaded from the Central Contractor Registry database. The G5 system is accessible to grantees to perform various transactions within their account to include, but not limited to, viewing grant award information and requesting grant payments. Because the DUNS number is

---

<sup>25</sup> Central Contractor Registration is the primary registrant database for the U.S. Federal Government that is used to collect, validate, store, and disseminate data in support of Federal agency assistance awards.

linked to each grantee's profile, an incorrect DUNS reassignment results in a grantee's profile, including grant award information, being exposed to an unauthorized grantee.

NIST SP 800-53, Revision 3, requires agencies to establish adequate system controls to promote the separation of duties to include mission functions, to ensure that distinct information system support functions are divided among different individuals or roles. NIST 800-53 also requires that different individuals perform information system support functions (for example, system management, systems programming, configuration management, quality assurance and testing, and network security). Further, NIST requires agencies to develop, disseminate, review, and update formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

The lack of effective controls for reassigning DUNS numbers resulted in an improper payment and in two grantees gaining access to each other's awards in the G5 system. Without monitoring controls of the DUNS reassignment process, the Department could incorrectly release more funds to grantees. Inadequate controls may cause grantees to question the integrity and accuracy of the grant issuance process. Although we reviewed only one improper payment that resulted from inadequate controls, the possibility exists that more improper payments could occur if monitoring controls are not implemented.

## **RECOMMENDATIONS**

We recommend that OCIO:

- 7.1 Develop a second-level review of DUNS changes to ensure that the DUNS reassignments are accurate and notify FSA of potential data errors.

### **Management Response**

OCIO concurred with Recommendation 7.1 and did not concur with Recommendation 7.2. For Recommendation 7.2, OCIO stated there is no logical approach or a DUNS hierarchy to programmatically connect the old and new DUNS by name, address, or other common factors in G5. Attempts to validate the reassignment programmatically by architecting an algorithm can yield flags to trigger the review of requests, or potentially accept invalid changes with no review. Therefore, implementing Recommendation 7.1 will result in full review of every payee DUNS change request.

### **OIG Response**

We removed draft Recommendation 7.2 in response to OCIO's comments.

## Appendix A: Objectives, Scope, and Methodology

The OIG contracted with Williams, Adley & Company, LLP, to conduct an independent information security system audit of EDCAPS. This audit helps fulfill the OIG's responsibilities related to FISMA, to conduct a comprehensive and independent information technology system security audit to determine the effectiveness of the Department's overall information security program and practices for the EDCAPS system.

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 OMB.

FISMA delegates to OMB and 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 perform an independent review or audit of the security controls in each application at least every 3 years. OCIO must establish and maintain information and information systems security controls for EDCAPS that are compliant with Federal laws, regulations, and standards.

### Objectives

The objective was to determine whether information technology security controls and effective management controls are in place to protect Departmental resources, including safeguarding personally identifiable information.

This audit was conducted in accordance with *Government Auditing Standards*, July 2007 Revision.<sup>26</sup> *Government Auditing Standards* required 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.

---

<sup>26</sup> The Government Accountability Office updated the *Government Auditing Standards* in December 2011. According to the Government Accountability Office, the 2011 revision of *Government Auditing Standards* was effective for financial audits and attestation engagements for periods ending on or after December 15, 2012, and for performance audits beginning on or after December 15, 2011. This audit began before December 15, 2011. Early implementation was not permitted.

## Scope

The scope of the audit included:

- The audit period of October 1, 2011, through March 30, 2012.
- An assessment of the OCIO management oversight controls of Dell's information security program for compliance with FISMA.
- Assessment of Department and EDCAPS policies, procedures, and controls against NIST Federal Information Processing Standard Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006; NIST SP 800-37, Revision 1, "Guide For Applying The Risk Management Framework To Federal Information Systems," February 2010; NIST SP 800-39, "Managing Information Security Risk," March 2011; NIST SP 800-61 "Computer Security Incident Handling Guide," March 2008; NIST SP 800-52, "Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations," June 2005; NIST SP 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," August 2009; NIST SP 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems," February 2006; and NIST SP 800-70, Revision 2, "National Checklist Program for IT Products – Guidelines for Checklist Users and Developers," February 2011.
- Assessment of the effectiveness of the Department's management oversight controls as required by OMB Circular A-130 and NIST Federal Information Processing Standards Publication 140-2 and FISMA.
- Tests of select general and application controls, and key management oversight controls, agreed upon by the OIG.
- Performance of detailed security reviews of designated information systems and applications by conducting vulnerability assessments and limited penetration testing of EDCAPS.
- Tests at the Department's headquarters located in Washington, D.C., and associated network hardware and software located at Dell's Plano, Texas data processing facility.

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 recertifications)
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. 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 a security review and tests of EDCAPS by conducting vulnerability assessments and penetration testing.
2. We tested to the levels necessary to determine the effectiveness of the EDCAPS controls to protect and secure Department data and to prevent potential advanced and persistent threats to the Department’s network architecture.

During our fieldwork, we engaged in many discussions with applicable Department officials and staff, including senior OCIO management, FMSS officials, CPSS officials, and G5 officials, to clarify the weaknesses noted and to provide clarification on recommendations. We also provided documents and other material produced during the network scans and vulnerability tests to OCIO and program officials for their review and action.

## Appendix B: EDCAPS System Description

### Components of EDCAPS

The EDCAPS Systems Security Plan states that EDCAPS has four components; however, in the previous OIG audit (EDUCATE) during fiscal year 2011, we found that e-Grants was combined with GAPS to create G5. Therefore, we evaluated the following three components of the EDCAPS major application.

Component Name	Brief Description
<b>Financial Management System Software</b>	FMSS provides functionality for general ledger and funds management, which includes budget formulation, budget execution, funds control, and the related internal and external reporting, including the financial statements. Also, FMSS includes receipt management, payments management for administrative funds, and funds availability checks.
<b>Contracts and Purchasing Support Software</b>	CPSS supports the preaward and postaward process for all types of contracts, delivery orders, task orders, interagency agreements, small purchases, and purchase card transactions. CPSS also interfaces with FMSS at the detail level for funds control, general ledger, accounts payable, invoicing, receipts, and accounts receivable.
<b>Grants Management System</b>	<p>G5 is a combination of two Web-based applications, GAPS and e-Grants.<sup>27</sup> G5 serves as a customer database for EDCAPS and the central repository of recipients having a relationship with the Department (for example, receiving grants). It maintains core information about a recipient and tracks reference data to support information recipients (for example, countries, States, and congressional districts). G5 also allows readers to access all the Department's Web-based grant systems, which includes the following functionalities:</p> <ul style="list-style-type: none"> <li>• e-payment—Provides grantees the ability to request funds and adjusts expenditures between awards.</li> <li>• e-reader—Allows peer reviewers to electronically review any application submitted electronically to the Department in their homes or offices.</li> <li>• e-reports—Provides the ability to prepare and submit Annual Grant Performance Reports to the Department via the Internet.</li> </ul>

---

<sup>27</sup> GAPS supports grant planning preaward, award management, and postaward of Department programs including discretionary, formula, fellowship, and block grants. The e-Grants system allows users to access all of the Department's Web-based grant systems that include Electronic Grant Application System (e-Application), a Web-based application for preparing and submitting a grant application electronically.



### *Platforms and Hardware*

The majority of EDCAPS hardware is physically stored in Plano, Texas. Also, the EDCAPS team has root access to the EDCAPS AIX servers. Dell has administrative rights to the Windows production servers.

The EDCAPS application is administered through Windows and AIX servers. According to the EDCAPS Systems Security Plan, the current EDCAPS server production architecture resides on IBM AIX operating system. The multi-tier environment is composed of dual load balanced Oracle Forms and Application Servers, and a three node Oracle Real Application Clusters. In addition to the Oracle backend, there is a Microsoft/Windows client server architecture consisting of Windows servers as the front-end, as well as Windows servers used in Single Sign-On architecture.

All EDCAPS servers, databases, application software, and data repository reside behind and are protected by firewalls under the control of EDUCATE. Routers and switches are deployed to control the Department's network entry and exit points.

### *Users*

The EDCAPS Systems Security Plan states EDCAPS serves about 2,500 internal users at the Department's headquarters and 21,000 external users across the nation and worldwide. The non-Department external users have access only to the Web-based application, G5. However, the internal users require both an EDUCATE user account, as well as an EDCAPS application user account to access EDCAPS applications.

## Appendix C: Office of Chief Information Officer Comments



### UNITED STATES DEPARTMENT OF EDUCATION


OFFICE OF THE CHIEF INFORMATION OFFICER

THE CHIEF INFORMATION OFFICER

#### MEMORANDUM

DATE: August 3, 2012

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

FROM: Danny A. Harris, Ph.D. 

SUBJECT: Education Central Automated Processing System (EDCAPS) Information Security Audit ED-OIG/A11M0002 Report Response

Thank you for the opportunity to address the recommendations in the draft Office of Inspector General's (OIG) report, Education Central Automated Processing System (EDCAPS) Information Security Audit ED-OIG/A11M0002. Your draft audit report provides valuable insight into the effectiveness of the information systems security controls in place to secure EDCAPS and accurately identifies several areas of needed improvement. The Office of the Chief Information Officer (OCIO) appreciates the attention provided by this report, and will work closely with your office to manage the response activities appropriately.

The following OCIO responses address each recommendation:

#### Risk Management Framework Needs Improvement

**OIG Recommendation 1.1** We recommend that OCIO improve the risk management framework by creating a review process where the implementation of a new system or the change to an existing system requires concurrence by upper management with the systems owner's risk assessment.

**Management Response:** OCIO partially concurs with this recommendation. OCIO agrees that the execution of the risk management framework can be improved, but the recommended review process already exists. OCIO has a review process in which the implementation of a new system, or a change to an existing system, requires review and approval by levels of management, based on the results of a risk assessment. This process is outlined in the Department's Information System Security Authorization Guidance, and it is integrated with the Department's Life Cycle Management process. While the review process exists, OCIO recognizes that improvements can be made in the execution of the risk management framework. OCIO has requested additional funding in fiscal year 2014 to make the Department's risk

400 MARYLAND 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.

management framework more robust and pro-active in terms of detailed reviews, quality, and effectiveness.

**OIG Recommendation 1.2** Perform and document a risk assessment for G5 Phase 3 and update, approve, and date the necessary documents.

**Management Response:** OCIO partially concurs with this recommendation. Prior to EDCAPS G5, Phase 2 becoming operational, OCIO performed and completed the required certification and accreditation of the system and granted an Authority To Operate (ATO) for G5 Phase 2. Since the G5 Phase 3 release included only changes to the business functionality, and not the IT infrastructure, it was determined by Information Assurance Services (IAS), and noted in the proceedings of the Enterprise Architecture Review Board (EARB), that new risk assessment documents were not required at that time. As per departmental Information System Security Authorization Guidance (Version 1.0, June 15, 2011), to maintain the existing EDCAPS ATO, the annual security assessment for EDCAPS, which includes G5, will be completed by September 30, 2012.

**OIG Recommendation 1.3** Complete the security authorization process and submit an updated ATO letter for G5 Phase 3.

**Management Response:** OCIO concurs with this recommendation. As per the departmental Information System Security Authorization Guidance (Version 1.0, June 15, 2011), to maintain the existing EDCAPS ATO, the annual security assessment for EDCAPS, which includes G5, will be completed by September 30, 2012.

#### Patch Management Needs Improvement

**OIG Recommendation 2.1** Require Dell and other contractors to comply with already agreed-on SLA requirements to install the security patches as soon as the patches are available from the manufacturer and after the patches have been properly tested to ensure patches do not adversely affect the system. The timeframe for testing and implementing patches should not exceed the required timeframes noted in the OCIO-01 Handbook.

**Management Response:** OCIO concurs with this recommendation. OCIO Information Technology Services (ITS) and Financial Systems Services (FSS) will identify and enforce the correct Service Level Agreements (SLAs), and the Services and Deliverables provisions, to ensure the Patch Management Standard Operating Procedures (SOPs) are followed. ITS and FSS will also revisit their patch management SOPs to ensure that they adhere to required patching timeframes, and that timeframes for testing and implementing patches do not exceed those noted in the OCIO-01, "Handbook for Information Assurance Security Policy." Corrective action by a specific date is not applicable.

**OIG Recommendation 2.2** Enforce the disincentive contract clauses for Dell and other contractors for not meeting the provision in the SLA to timely implement patches.



**Management Response:** OCIO concurs with this recommendation. Going forward, OCIO ITS and FSS will identify and enforce appropriate disincentives for contractors and contracts not meeting the Service Level Agreements (SLAs), and the Services and Deliverables provisions for timely implementation of patches. Corrective action by a specific date is not applicable.

**OIG Recommendation 2.3** Immediately correct or mitigate the vulnerabilities identified.

**Management Response:** OCIO concurs with this recommendation. The FSS team has already addressed many of the specific audit report vulnerabilities cited (see Attachment). FSS will create a Plan of Actions and Milestones (POA&M) for each of the unresolved vulnerabilities identified in the audit report by November 30, 2012.

#### EDCAPS Security Configuration Management Controls Needed Improvement

**OIG Recommendation 3.1** Implement an enterprise approach with established implementation dates to enforce mandatory security configuration settings for the EDCAPS system and all other Department systems. OCIO and Dell should document all agreed on implementation dates for fixing all enterprise-wide patching and configuration vulnerabilities.

**Management Response:** OCIO partially concurs with this recommendation. The proposed recommendation discusses two concepts: (1) an enterprise approach to enforce mandatory security configuration settings, and (2) OCIO/Dell agreement on implementation dates for enterprise-wide patches and vulnerabilities. With respect to an enterprise approach to enforce mandatory security configuration settings, OCIO has published Information Technology Security Configuration Management Guidance, dated February 20, 2009, which states, "All ED information system owners will ensure their systems undergo a baseline security configuration validation on an annual basis" and provides guidelines for ensuring compliance. This guidance and the Department's security authorization and POA&M processes comprise our enterprise approach to enforcing mandatory security configuration settings. While an enterprise approach exists, OCIO recognizes that improvements can be made in the execution of the Department's configuration management control. OCIO has requested additional funding in fiscal year 2014 to make the Department's risk management framework and patch and vulnerability management processes more robust and pro-active.

OCIO ITS and FSS will work with the appropriate vendor(s) to document implementation dates for addressing all specific vulnerabilities identified within the audit report by September 30, 2012.

**OIG Recommendation 3.2** Establish reporting procedures to monitor Dell's monthly progress to ensure identified vulnerabilities are fixed within the established timelines.

**Management Response:** OCIO partially concurs with this recommendation. OCIO IAS already monitors the EDUCATE program's progress toward remediating identified vulnerabilities, as with all other programs, through the Department's Operational Vulnerability

Management System (OVMS) and the tracking of open POA&Ms in accordance with the timelines established in the Department “Plan of Actions and Milestones Guidance.” OCIO recognizes that improvements can be made in the reporting and tracking of vulnerabilities, and their remediation, and will work with Dell to continually enhance the existing reporting and monitoring processes. Corrective action by a specific date is not applicable.

#### Keylogger Incident Reporting for G5 Needs Improvement

**OIG Recommendation 4.1** We recommend that OCIO revise the OCIO-14 Handbook to require the Education Incident Response Coordinator Team to enter all keylogger incidents reported by USCERT into OVMS and use OVMS to review, reconcile, track, report, and resolve the all keylogger incidents, not just G5.

**Management Response:** OCIO concurs with this recommendation. The Education Cyber Incident Response Center (EDCIRC) conducted a thorough review of the most recently published version of OCIO-14, “Handbook for Information Security Incident Response and Reporting Procedures,” which showed that the document needs additional focus and revision. OCIO IAS and EDCIRC are in the process of revising OCIO-14 to clearly delineate the roles and responsibilities of Department employees and contractors in relationship to the actor’s involvement in a computer-related incident. These revisions will include requirements that all keylogger incidents reported, both from US CERT and other outside sources, be entered into the OVMS Incident Response Tracking Module (IRTM) module. IAS will submit the final revisions to OCIO-14 through the Administrative Communications System team for final approval by second quarter Fiscal Year (FY) 13.

#### Configuration Management Database Is Not Properly Maintained

**OIG Recommendation 5.1** Enforce SLA requirements requiring Dell to implement procedures to update the Department’s Asset Management System of Record and to reconcile it with Dell’s inventory management system data at least once a month.

**Management Response:** OCIO partially concurs with this recommendation. To date, there are no SLA requirements in the EDUCATE contract that require Dell to implement procedures to update the Department’s Asset Management System or the Configuration Management Database. OCIO ITS continues to work with Dell to improve upon procedures to update and reconcile the Department’s assets. Corrective action by a specific date is not applicable.

**OIG Recommendation 5.2** Enforce the disincentive contract clauses for Dell and other contractors for not implementing the procedures to update the Department’s Asset Management System of Record and not reconciling the record with the Contractor’s inventory management system, according to the timelines specified in the SLA.



**Management Response:** OCIO partially concurs with this recommendation. To date, there are no SLA requirements in the EDUCATE contract that require Dell to implement procedures to update the Department's Asset Management System. OCIO ITS will continue to monitor compliance with asset management requirements, and will apply the appropriate penalties when justified. Corrective action by a specific date is not applicable.

**OIG Recommendation 5.3** Require the Information Technology Services Group to perform a review and reconciliation of hardware to ensure the information Dell reports is accurate.

**Management Response:** OCIO concurs with this recommendation. OCIO ITS will develop a review and reconciliation procedure of the hardware to ensure the information Dell reports is accurate by September 30, 2012.

#### The Department Has Not Implemented a Security Configuration Baseline

**OIG Recommendation 6.1** Expedite the review and approval of the draft baseline configuration documents.

**Management Response:** OCIO partially concurs with this recommendation. OCIO IAS published the "Information Technology Security Baseline Configuration Guidance" on February 20, 2009. This guidance document requires system owners to ensure their systems undergo a baseline security configuration validation. This document also specifies that IT system owners will ensure compliance with established baseline configuration standards of the NIST National Checklist Program. For IT systems that have components not addressed within the NIST National Checklist Program, a benchmark from the Center for Internet Security (CIS) can be used (i.e. Mac and Linux). If an IT system has components not addressed by either of the former configuration standards, component vendor security and/or industry best practice security configurations must be employed. OCIO recognizes that improvements can always be made in the execution of the Department's security configuration baseline controls establishment and oversight processes and will endeavor to make these enhancements. Corrective action by a specific date is not applicable.

**OIG Recommendation 6.2** Provide an alternate or acting position for the vacant Information Security Manager's position to approve the draft baseline configuration documents and maintain up-to-date baseline configuration documentation with vendor and Department specifications and changes.

**Management Response:** OCIO concurs with this recommendation. The Systems Operations and Maintenance Team (SOMT) manager within FSS is acting as the EDCAPS Information Systems Security Officer (ISSO) until the ISSO vacancy is filled. The acting EDCAPS ISSO will review and approve the draft EDUCATE configuration baseline documentation in accordance with the NIST SP 800-53, Revision 3 Guidance and the OCIO-11 Handbook, and maintain up-to-date baseline configuration documentation with vendor and Department

specifications and changes. The ISSO will sign the final baseline configuration document by September 30, 2012.

**OIG Recommendation 6.3** Establish procedures to effectively cross train OCIO personnel in all critical positions/functions to ensure workload and processes are not compromised when vacancies occur.

**Management Response:** OCIO concurs with this recommendation. OCIO recognizes the need to have backups for all critical positions/functions in the component offices. In addition to having designated and trained backups for these critical positions/functions, the OCIO is also working to populate a section of the OCIO Sharepoint webspace with Procedures That Work (PTW). PTWs are formatted narratives that explain how specific OCIO business processes are carried out. These procedures enable another member of the office staff, if someone is absent, to accomplish the process by following the instructions/guidance presented in the PTW for that business process. These PTWs will be accessible to OCIO staff and will provide another means of ensuring that a process or function can be carried out, in the event staff principally responsible for performing the process or function are unavailable.

#### Separation of Duties Needed for G5 Application Users

**OIG Recommendation 7.1** Develop a second-level review of DUNS changes to ensure that the DUNS reassignments are accurate and notify FSA of potential data errors.

**Management Response:** OCIO concurs with this recommendation. There is confusion between DUNS reassignment and a payee DUNS change request. The description of the issue is related to a payee DUNS change request, while the reference in the issue description and recommendation is related to a global DUNS reassignment. The G5 team has modified the payee DUNS change procedure to add a second functional user validation of payee DUNS change requests before they are updated in the system. The procedure has been in effect since June 4, 2012.

**OIG Recommendation 7.2** Implement G5 application-level edit checks ensuring that reassigned DUNS numbers entered into the G5 system match the intended grantee, and require a manual override for reassigned DUNS numbers that do not match the grantee.

**Management Response:** OCIO non-concurs with this recommendation. There is no logical approach or a DUNS hierarchy to programmatically connect the old and new DUNS by name, address, or other common factors in G5. Attempts to validate the reassignment programmatically by architecting an algorithm can yield flags to trigger the review of requests, or potentially accept invalid changes with no review. Therefore, implementing recommendation 7.1 will result in full review of every payee DUNS change request.



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

Attachment

## Responses for EDCAPS G5 Patch Management Findings

### 2.3 A Use of software that is no longer supported by vendors or not installing current patches.

- The Technology Levels (that is, versions) of 16 production AIX (UNIX) systems were not up to date. These systems are missing critical security patches.

**Concur.** The missing patches were applied on July 16, 2012.

- Six production UNIX systems are running versions of IBM WebSphere Application server that are multiple versions behind the current release, making the systems vulnerable to multiple application-level attacks. The fix pack installed is number 33 (released February 13, 2009) instead of the current fix pack 43 (released September 27, 2010).

**Concur.** The updates were installed on July 16, 2012.

- Three G5 production Apache Web servers are vulnerable to denial-of service attacks and another G5 production server is vulnerable to buffer overflow attacks. The Apache Web servers do not have the latest patches.

**Concur.** The updates were installed on July 16, 2012.

- The Cognos Web application has an unsupported version of Internet Information Services Web server, Adobe Reader, and Microsoft Office. These unsupported versions make the system vulnerable to attacks.

**Concur.** The server is scheduled to be decommissioned by July 31, 2012.

- One server is running the Windows 2000 operating system, which Microsoft no longer supports. Microsoft will not release security patches and other software fixes for Windows 2000, making this server more vulnerable to attacks.

**Concur.** The server is scheduled to be decommissioned by July 31, 2012.

### 2.3 B G5 Database Vulnerabilities.

- Three critical vendor security patches (released by the vendor more than three months from the time of testing) for two Oracle databases have not been installed, making them susceptible to cyber-attacks. We previously identified the security patches condition during the fiscal year 2011 EDUCATE and the FISMA audits.

**Concur.** EDCAPS has planned to perform this effort as part of its quarterly release in November 2012.

- One Oracle database is missing critical patch updates dating back to April 2011, and another Oracle database is missing the most recent patchset.<sup>12</sup> This is a modified repeat condition, similar to the security patch weaknesses identified in the fiscal year 2011 OIG audit reports for EDUCATE and FISMA.

**Concur.** EDCAPS has planned to perform this effort as part of its quarterly release in November 2012.

- Two Oracle databases have the remote login password file enabled, which does not provide a lockout feature and is potentially vulnerable to password attacks.

**Partially-Concur.** The EDCAPS database uses the Oracle Data Guard feature, which requires that the remote login password file be enabled. However, for the CEDCAPS database, we plan to implement this change with the quarterly release in November 2012.

- Two Oracle databases give the PUBLIC role EXECUTE privilege on the SYS.UTL\_FILE, which potentially allows Procedural Language/Structured Query Language<sup>13</sup> to read from and write to files on the operating system.

**Concur.** EDCAPS has planned to perform this effort as part of its quarterly release in November 2012.