



DEPARTMENT OF EDUCATION INCLUDING DIRECT AID TO PUBLIC EDUCATION

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2019

Auditor of Public Accounts
Martha S. Mavredes, CPA
www.apa.virginia.gov
(804) 225-3350



AUDIT SUMMARY

Our audit of the Department of Education and Direct Aid to Public Education; collectively referred to as “Education” throughout this report, for the fiscal year ended June 30, 2019 found:

- proper recording and reporting of all transactions, in all material respects, in the Commonwealth’s accounting and financial reporting system, Education’s financial system, and in attachments submitted to the Department of Accounts;
- an issue that is beyond the corrective action of Education’s management and requires the cooperation of the Virginia Information Technologies Agency to address the risk, which we report as a “Risk Alert;”
- matters involving internal control and its operation necessary to bring to management’s attention;
- instances of noncompliance with the Commonwealth’s standards related to information technology; and,
- with the exception of one information security audit finding, adequate corrective action with respect to audit findings reported in the prior year.

- TABLE OF CONTENTS -

	<u>Pages</u>
AUDIT SUMMARY	
INTERNAL CONTROL AND COMPLIANCE RISK ALERT	1-2
INTERNAL CONTROL AND COMPLIANCE RECOMMENDATIONS	2-3
INDEPENDENT AUDITOR'S REPORT	4-7
AGENCY RESPONSE	8-9
AGENCY OFFICIALS	10

INTERNAL CONTROL AND COMPLIANCE RISK ALERT

What is a Risk Alert

During the course of our audit, we encountered an internal control and compliance issue that is beyond the corrective action of Education's management alone and requires the action and cooperation of management and the Virginia Information Technologies Agency (VITA). The following issue represents a risk to Education and the Commonwealth during fiscal year 2019.

Improve Vulnerability Remediation Efforts

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

Education relies on VITA's contractual partnership with various information technology (IT) service providers (Partnership) to install, maintain, operate, and support IT infrastructure components, such as servers, routers, firewalls, and virtual private networks. As a part of these services, Education relies on the Partnership to install security patches and updates to software to remediate weaknesses found in vulnerability scans.

During our review, we found that the Partnership is not installing certain security patches for Education's systems to remediate vulnerabilities. The Partnership states it does not support certain software maintained for Education's systems and that it is the responsibility of Education to maintain the software. However, Education does not have the ability to install patches for its systems because only the Partnership has administrative privileges to the servers. Additionally, VITA does not have a list of approved software to provide Education so the agency knows what software the Partnership will support.

The Commonwealth's IT Risk Management Standard, SEC 520 (IT Risk Management Standard), Section 3.7 *Vulnerability Scanning*, requires vulnerability scans be performed at least once every 90 days and when new vulnerabilities potentially affecting the system or application are identified and reported. Additionally, legitimate vulnerabilities are required to be remediated within 90 days based on risk. Furthermore, the Commonwealth's Information Security Standard, SEC 501 (Security Standard), section SI-2 *Flaw Remediation*, requires security-relevant software and firmware updates be installed within 90-days of the release of the update.

With the Partnership not installing certain security patches and updates, it increases the risk of cyberattack, exploit, and data breach by malicious parties. Education is aware of this issue and is working with the Partnership to develop remediation plans to install security patches and updates in accordance with the Security Standard. Additionally, the Commonwealth Security and Risk Management group within VITA is aware of the need to publish a list of approved software the Partnership will support.

Education should continue working with the Partnership to install current security patches and updates for its IT systems and workstations to remediate vulnerabilities and maintain up-to-date software. Additionally, VITA should develop and publish a list of approved software so Education is aware of the software the Partnership supports. Doing this will further reduce the risk to the confidentiality, integrity, and availability of sensitive Commonwealth data and achieve compliance with the Security Standard and IT Risk Management Standard.

INTERNAL CONTROL AND COMPLIANCE RECOMMENDATIONS

Why the APA Audits Information Security

Education is responsible for managing state and federal appropriations that support public instruction. During fiscal year 2019, Education expended approximately \$8 billion, most of which was disbursed to local school divisions. In addition, Education is responsible for ensuring that personally identifiable information for students and teachers is protected. Education's IT systems and practices are critical for accomplishing these business objectives. To ensure that Education's IT general and application controls are effectively designed in accordance with the Security Standard; IT Risk Management Standard; the Commonwealth's IT Security Audit Standard, SEC 502; and industry best practices, we performed testwork over the policies, procedures, and security controls supporting Education's IT environment.

Implement Process for Ongoing Monitoring of System Access

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

Education did not remove temporary elevated access to an employee for the School Nutrition Programs web application (web application). During our review of web application access, we found that one employee of the six tested (17%) inappropriately retained access that allowed the employee to modify and submit annual agreements, as well as provide first and second levels of approval for annual agreements.

The Security Standard, Section AC-6: Least Privilege, states; "the organization employs the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions." The program specialist with extended access could have potentially modified and approved changes for the following year to the meal programs in which local school divisions participated, violating the established controls governing the web application.

In this case, Education intended to temporarily grant the employee elevated access; however, Education did not reduce the employee's access rights after their task was completed. Additionally, Education does not have a review process in place to evaluate the reasonableness of access when it changes responsibilities for an employee. As a result, Education should develop formal policies and procedures for ongoing monitoring of existing user access to ensure the principle of least privilege is maintained.

Continue Improving Database Security

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Yes (first issued in fiscal year 2016)

Education continues to make progress to improve a security control for its database that stores its financial activity in accordance with the Security Standard. We communicated the remaining control weakness to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. Since the prior year audit, Education is actively working with the Commonwealth's IT Partnership to implement a solution and resolve the weakness. The Security Standard requires agencies to implement certain controls that reduce unnecessary risk to data confidentiality, integrity, and availability in systems processing or storing sensitive information. By not meeting the minimum requirements in the Security Standard, Education cannot ensure the confidentiality, integrity, and availability of data within the database or the information it reports.

Education should continue working with the Partnership to implement the control discussed in the communication marked FOIAE in accordance with the Security Standard and in a timely manner.

Improve Web Application Security

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

Education does not configure a sensitive web application in accordance with the Security Standard. We identified three control weaknesses and communicated them to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia, due to it containing description of security mechanisms. The Security Standard requires agencies to implement certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of Education's information systems and data.

Education took immediate corrective action to subsequently resolve two of the three weaknesses included in the FOIAE document. Education should develop a plan to implement the remaining control included in the communication marked FOIAE in accordance with the Security Standard and in a timely manner. Doing this will help to ensure Education secures the web application to protect its sensitive and mission critical data.



Martha S. Mavredes, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 13, 2019

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Thomas K. Norment, Jr.
Chairman, Joint Legislative Audit
and Review Commission

We have audited the financial records and operations and federal compliance of the **Department of Education including Direct Aid to Public Education** (Education) for the year ended June 30, 2019. We conducted this audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, in support of the Commonwealth's Annual Financial Report and Single Audit. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Objectives

Our audit's primary objective was to evaluate the accuracy of Education's financial transactions as reported in the Comprehensive Annual Financial Report for the Commonwealth of Virginia and test federal compliance in support of the Commonwealth's Single Audit, both for the year ended June 30, 2019. In support of this objective, we evaluated the accuracy of recorded financial transactions in the Commonwealth's accounting and financial reporting system, Education's financial system, and in attachments submitted to the Department of Accounts (Accounts); reviewed the adequacy of Education's internal control; tested for compliance with applicable laws, regulations, contracts, and grant agreements; and reviewed corrective actions with respect to audit findings from prior year reports.

Audit Scope and Methodology

Education's management has responsibility for establishing and maintaining internal control and complying with applicable laws, regulations, contracts, and grant agreements. Internal control is a process designed to provide reasonable, but not absolute, assurance regarding the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws, regulations, contracts, and grant agreements.

We gained an understanding of the overall internal controls, both automated and manual, sufficient to plan the audit. We considered materiality and risk in determining the nature and extent of our audit procedures. Our review encompassed controls over the following major programs, significant cycles, classes of transactions, and account balances.

Federal grants management for:

- Title I Grants to Local Education Agencies – Catalog of Federal Domestic Assistance (CFDA) 84.010
- Improving Teacher Quality State Grants – CFDA 84.367
- Child Nutrition Cluster – CFDA 10.553, 10.555, 10.556, and 10.559
- Special Education Cluster Individuals with Disabilities Education Act (IDEA) – CFDA 84.027 and 84.173

Standards of Quality allocations and disbursements to localities

Appropriations

Accounts receivable

Accounts payable

Authorizations of Virginia Public School Authority Education Technology grant payments

Information system security to include:

- Systems and data security
- Security awareness and training
- Security audits
- Risk assessments

We performed audit tests to determine whether Education's controls were adequate, had been placed in operation, and were being followed. Our audit also included tests of compliance with provisions of applicable laws, regulations, contracts, and grant agreements. Our audit procedures included inquiries of appropriate personnel, inspection of system access, documents, records, journal entries, and contracts, and observation of Education's operations. We performed analytical procedures, including trend and appropriation analyses. We also tested details of transactions, along with reconciliations of financial, accounting, and management systems to achieve our objectives.

A nonstatistical sampling approach was used. Our samples were designed to support conclusions about our audit objectives. An appropriate sampling methodology was used to ensure the samples selected were representative of the population and provided sufficient, appropriate evidence. We identified specific attributes for testing each of the samples and when appropriate, we projected our results to the population.

Our consideration of internal control over financial reporting and federal compliance was for the limited purpose described in the section “Audit Objectives” and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and; therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control we consider to be material weaknesses. We did identify certain deficiencies in internal control that we consider to be significant deficiencies, which are described in the sections titled “Internal Control and Compliance Risk Alert” and “Internal Control and Compliance Recommendations.”

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements or noncompliance on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity’s financial statements or material noncompliance with a type of compliance requirement for a federal program will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Conclusions

We found that Education properly stated, in all material respects, the amounts recorded and reported in the Commonwealth’s accounting and financial reporting system, Education’s financial system, and in attachments submitted to Accounts, including federal schedules.

We noted certain matters involving internal control and its operation and compliance with applicable laws, regulations, contracts and grant agreements that require management’s attention and corrective action. These matters are described in the sections titled “Internal Control and Compliance Risk Alert” and “Internal Control and Compliance Recommendations.”

Education has not completed corrective action with respect to the previously reported finding titled “Continue Improving Database Security.” Accordingly, we included this finding in the section entitled “Internal Control and Compliance Recommendations.” Apart from this finding, Education has taken adequate corrective action, including implementing compensating controls, with respect to the other audit findings that were reported in the prior year that are not repeated in this letter.

Since the findings noted above include those that have been identified as significant deficiencies, they will be reported as such in the “Independent Auditor’s Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of the Financial Statements Performed in Accordance with Government Auditing Standards” and the “Independent Auditor’s Report on Compliance for Each Major Federal Program; Report on Internal Control over Compliance; and Report on Schedule of Expenditures of Federal Awards Required by Uniform Guidance,” which are included in the Commonwealth of Virginia’s Single Audit Report for the year ended June 30, 2019. The Single Audit Report will be available at www.apa.virginia.gov in February 2020.

Exit Conference and Report Distribution

We discussed this report with Education’s management on January 21, 2020 and have included their response at the end of this report in the section titled “Agency Response.” We did not audit management’s response and, accordingly, we express no opinion on the response. Additionally, on January 24, 2020 we provided management of the Virginia Information Technologies Agency (VITA) with a copy of the Risk Alert titled “Improve Vulnerability Remediation Efforts” for their response. VITA’s management elected not to provide a response for inclusion in the audit report.

This report is intended for the information and use of the Governor and General Assembly, management, and the citizens of the Commonwealth of Virginia and is a public record.

Martha S. Mavredes
AUDITOR OF PUBLIC ACCOUNTS

GDS/clj



COMMONWEALTH of VIRGINIA

James F. Lane, Ed.D.
Superintendent of Public Instruction

DEPARTMENT OF EDUCATION
P.O. BOX 2120
Richmond, Virginia 23218-2120

Office: (804) 225-2023
Fax: (804) 371-2099

January 27, 2019

Ms. Martha Mavredes
Auditor of Public Accounts
Post Office Box 1295
Richmond, Virginia 23218-1295

Dear Ms. Mavredes:

I appreciate the opportunity to respond to the findings of the audit completed by the Auditor of Public Accounts of the Department of Education (DOE) and Direct Aid to Public Education, for the fiscal year ended June 30, 2019. I am pleased that the audit found that the Department properly recorded and reported all transactions, in all material respects, in the Commonwealth's financial reporting system. The audit did note matters involving internal control and its operations and compliance with applicable laws, regulations, contracts and grant agreements that require DOE's attention and corrective action. The report contains recommendations for improvement that will focus the work of the agency's management and staff who will implement them.

Regarding the findings related to the *Risk Alert – Improve Vulnerability Remediation Efforts*, agency management recognizes the concerns outlined in the report. DOE will continue to work with the Partnership (i.e., Virginia Information Technologies Agency) to ensure that installation of current security patches and other updates for its IT systems and workstations are conducted. DOE will also monitor additional resources that may be provided by the Partnership in support of improving this area.

Regarding the findings related to the *Implementing Process for Ongoing Monitoring of System Access*, management is aware of the importance of removing temporary system access following the completion of tasks. In addition, management has begun developing formal policies and procedures for periodic monitoring of existing user access to ensure that accurate access and rights are maintained for systems in our School Nutrition Programs. Management would like to note that the system access in this case did not affect school divisions' previous

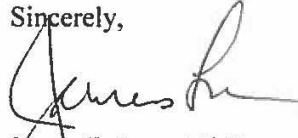
approvals for participation in particular school nutrition programs, nor the reimbursement rates for the programs in which they were approved to participate.

Regarding the findings related to the Continue Improving Database Security, management is aware of the importance of meeting the requirement in the Commonwealth Security Standard to ensure confidentiality, integrity and availability of data within the database or the information it reports. DOE has made significant improvements in database security since the previous audit. There is one control within database security that requires additional attention from DOE management related to the monitoring of audit logs of administrative users. DOE began working with the Partnership in February 2019 to acquire the log reports that are captured and controlled by the Partnership. After multiple attempts by DOE, which were unsuccessful, to obtain these reports from the Partnership, DOE has begun to pursue an alternative software through a 3rd party to report this information in order to achieve compliance with the Security Standard.

Regarding the findings related to the Improve Web Application Security, management would like to note that this particular finding was corrected during the course of the audit. DOE will ensure that this information remains in the corrected status for future reviews and audits.

Thank you for the opportunity to provide an agency response to the audit report. The Department of Education has made great strides to improve the work that is conducted within the agency over the course of the past year and is committed to focusing on the very important findings and recommendations identified as needing attention.

Sincerely,



James F. Lane, Ed.D.
Superintendent of Public Instruction

DEPARTMENT OF EDUCATION

As of June 30, 2019

AGENCY OFFICIAL

James F. Lane
State Superintendent of Public Instruction