# DEPARTMENT OF EDUCATION

# AND DIRECT AID TO PUBLIC EDUCATION

## REPORT ON AUDIT

## FOR THE YEAR ENDED

## JUNE 30, 2023


Auditor of Public Accounts
Staci A. Henshaw, 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, 2023, found:

- proper recording and reporting of all transactions, in all material respects, in the Commonwealth's accounting and reporting system, Education's financial system, and in attachments submitted to the Department of Accounts (Accounts);

- three matters involving internal control and its operation necessary to bring to management's attention that also represent instances of noncompliance with applicable laws and regulations or other matters that are required to be reported; and

- two issues that are beyond the corrective action of Education's management and require the cooperation of the Virginia Information Technologies Agency (VITA) to address the risks, which we report as "Risk Alerts."

We did not perform audit work on the prior audit finding titled "Ensure the Correct Award Year is Applied to Federal Reports" as noted in the Findings Summary included in the Appendix because Education did not implement corrective action during our audit period. Corrective action has been ongoing since the fiscal year 2022 audit. We will follow up on this finding during the fiscal year 2024 audit.

In the section titled "Internal Control and Compliance Findings and Recommendations" we have included our assessment of the conditions and causes resulting in the internal control and compliance findings identified through our audit as well as recommendations for addressing those findings. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the findings and developing and appropriately implementing adequate corrective actions to resolve the findings as required by the Department of Accounts in Section 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendations.

# -TABLE OF CONTENTS-

# INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

**Improve Vulnerability Management Process**
**Type:** Internal Control and Compliance
**Severity:** Significant Deficiency

Education does not consistently remediate vulnerabilities in its information technology (IT) environment within the timeframe required by agency policy and the Commonwealth's Information Security Standard, SEC 501 (Security Standard). VITA and Education share the responsibility for the remediation of legitimate vulnerabilities and Education does not consistently remediate vulnerabilities that are its responsibility. We communicated the weaknesses and recommendations 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.

Both Education's Information Security Policy Manual and the Security Standard require Education to remediate legitimate vulnerabilities within 90 days in accordance with an organizational assessment of risk. Without remediating vulnerabilities within the required timeframe, Education increases the risk of unauthorized access to the IT environment.

Education follows a vulnerability management process; however, some extensive and time-consuming elements of the process caused delays in remediation efforts. Education should improve its vulnerability management process to remediate vulnerabilities within the timeline required by the Security Standard and its Information Security Policy Manual. By remediating vulnerabilities timely, Education will reduce data security risks for sensitive and mission-critical systems and better protect the confidentiality, integrity, and availability of the data processed by those systems.

**Improve IT Risk Management Program**
**Type:** Internal Control and Compliance
**Severity:** Significant Deficiency

Education is missing certain elements within its IT risk management program to meet the requirements in the Commonwealth's Security Standard. We communicated the weaknesses and recommendations 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.

The Security Standard requires that Education review and update its risk assessment at least annually or when significant changes occur to the system or IT environment (Security Standard, Section 6.2 Risk Assessment). The Security Standard also requires that Education perform an initial risk analysis at project initiation for each external information system (Security Standard, Section SA-3-COV-1). Additionally, the Security Standard requires Education to develop a system security plan for the information system and conduct an annual review of the SSP (Security Standard, Section PL-2 System Security Plan).

Without conducting and annually reviewing its risk management documentation, Education increases the risk that it may not properly secure its sensitive systems. An unexpected delay in implementing the planned risk management solution contributed to Education not consistently maintaining its risk management documentation.

Education should complete the implementation of its new risk management solution. In addition, Education should conduct and annually review each element of its risk management documentation. This will help ensure the confidentiality, integrity, and availability of sensitive and mission-critical data.

**Improve Third-Party Service Provider Process**
**Type:** Internal Control and Compliance
**Severity:** Significant Deficiency

Education does not monitor the effectiveness of security controls of external service providers (providers) that fall under VITA's Enterprise Cloud Oversight Service (ECOS). Providers are organizations that perform outsourced business tasks or functions on behalf of Education and the Commonwealth. Education uses VITA's ECOS to assist the agency with gaining assurance that its providers implement the minimum-security controls required by the Commonwealth's Hosted Environment Security Standard, SEC 525 (Hosted Environment Security Standard). Education uses seven providers for mission-critical business functions that process and store sensitive data.

Specifically, Education does not have policies or procedures that assign roles and responsibilities to ensure that Education works with ECOS to receive and review communications from providers. As a result, our review identified the following weaknesses:

- Education does not receive and review monthly status reports that confirm the exact geographic location of data and provide vulnerability scan results for two of its seven providers.

- Education does not have a formal contractual agreement with one of its seven providers.

- Education does not identify subservice organizations that deliver or assist in the delivery of a service relied upon to support a provider's environment. Additionally, Education does not assess and document significant services provided by subservice organizations that require assurance of controls.

The Hosted Environment Security Standard, Section 1.1, states management remains accountable for maintaining compliance with the Hosted Environment Security Standard through documented agreements and oversight of services provided. Education procured multiple service providers in recent years and only recently prioritized establishing a formal service provider oversight process for existing providers and providers currently in procurement, which contributed to the weaknesses identified above.

Education should mature its policies and procedures to align with the Hosted Environment Security Standard and outline its requirements and processes for consistently maintaining ongoing oversight of its providers. By gaining assurance over the effectiveness of each provider's operating controls, Education will help to ensure the confidentiality, integrity, and availability of sensitive data.

## RISK ALERTS

During the course of our audit, we encountered issues that are beyond the corrective action of Education management alone and require the action and cooperation of management and VITA. The following issues represent such a risk to Education and the Commonwealth during fiscal year 2023.

**Unpatched Software**

**First Issued:** Fiscal Year 2019

VITA contracts with various providers to create the Commonwealth's Information Technology Infrastructure Services Program (ITISP) to provide agencies with installation, maintenance, operation, and support of IT infrastructure components, such as servers, routers, firewalls, and virtual private networks.

Education continues to rely on contractors procured by VITA for the installation of security patches in systems that support Education's operations. Additionally, Education relies on VITA as the contract administrator to maintain oversight and enforce the contract agreements with the ITISP contractors. As of July 2023, the ITISP contractors had not applied a significant number of security patches that are critical and highly important to Education's IT infrastructure components, all of which are past the 90-day update window allowed by the Commonwealth's Security Standard.

The Security Standard requires the installation of security-relevant software updates within 90 days of release. The Security Standard does allow for varying time periods depending on factors such as the criticality of the update, but generally the ITISP uses a 90-day window from the date of release as its standard for determining timely implementation of security patches (Security Standard, Section SI-2 Flaw Remediation). Missing system security updates increases the risk of successful cyberattack, exploit, and data breach by malicious parties.

While VITA is responsible for enforcing the service level agreement, it has not been able to compel the current ITISP contractors to install certain security patches to Education's IT infrastructure components to remediate vulnerabilities in a timely manner or taken actions to obtain these required services from another source. Education is working with VITA and the ITISP contractors to ensure that the ITISP contractors install all critical and highly important security patches on all servers. Additionally, our separate audit of VITA's contract management will also continue to report on this issue.

**Access to Audit Log Monitoring Tool**

**First Issued:** Fiscal Year 2020

Education relies on the ITISP to install, maintain, operate, and support IT infrastructure components, such as servers, routers, firewalls, and virtual private networks. As part of these services, Education relies on contractors procured by the VITA to provide Education access to a centralized monitoring tool, known as the Managed, Detection, Response (MDR) Dashboard, that collects audit log information about activities in Education's IT environment so that Education can review logged activity. Additionally, Education relies on VITA to maintain oversight and enforce the service level agreements and deliverables with the ITISP contractors.

While VITA did not originally enforce the deliverable requirement when ratifying the ITISP contracts in 2018, VITA tried to compel the ITISP contractor to grant agencies, such as Education, access to the monitoring tool and audit log information for the last four years. As of October 2023, the MDR Dashboard became available for agencies to use for monitoring purposes. However, while Education received access to the MDR Dashboard during the pilot program, the MDR Dashboard does not include all audit log information to allow agencies to adequately monitor their IT environments. Additionally, VITA and the ITISP contractor have not provided training to agencies on how to use the MDR Dashboard.

The Security Standard requires a review and analysis of audit records at least every 30 days for indications of inappropriate or unusual activity (Security Standard, Section AU-6 Audit Review, Analysis, and Reporting). VITA not enforcing the deliverable requirements from the ITISP contractors increases the risk associated with the Commonwealth's data confidentiality, integrity, and availability.

Education is working with VITA and VITA's ITISP contractors on how to utilize the MDR Dashboard and verify the inclusion of all audit log information to ensure Education can review the activities occurring in its IT environment in accordance with the Security Standard. Additionally, our separate audit of VITA's contract management will also continue to report on this issue.

Commonwealth of Virginia

*Auditor of Public Accounts*

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 15, 2023

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Lisa Coons, Superintendent of Public Instruction
Department of Education

We have audited the financial records, operations, and federal compliance of the **Department of Education including Direct Aid to Public Education (Education)** for the year ended June 30, 2023. 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 Comprehensive 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 Annual Comprehensive Financial Report for the Commonwealth of Virginia and test federal compliance in support of the Commonwealth's Single Audit for the year ended June 30, 2023. 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 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 risk alerts 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 federal programs, significant cycles, classes of transactions, and account balances.

Federal grants management for the following programs:

- Child and Adult Care Food Program – Assistance Listing Number (ALN): 10.558
- Coronavirus State and Local Fiscal Recovery Funds – ALN: 21.027
- Education Stabilization Fund – ALN: 84.425

Standards of Quality allocations and disbursements to localities

Appropriations

Accounts receivable

Accounts payable

Information system security to include:

- Database security
- IT change control and configuration management
- IT risk management
- IT vulnerability and patch management
- Third-Party Service Provider Oversight
- VITA/ITISP services

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 documents, records, and contracts, and observation of Education's operations. We performed analytical procedures, including budgetary and trend analyses, and tested details of transactions to achieve our audit 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 (internal control) 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 that we consider to be material weaknesses. We did identify certain deficiencies in internal control titled "Improve Vulnerability Management Process," "Improve IT Risk Management Program," and "Improve Third-Party Service Provider Process," which are described in the section titled "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies.

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 of 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 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 section titled "Internal Control and Compliance Findings and Recommendations."

We did not perform audit work related to the finding included in our report dated December 15, 2022, titled "Ensure the Correct Award Year is Applied to Federal Reports," because Education did not implement corrective action during our audit period. We will follow up on this finding during the fiscal year 2024 audit.

Since the findings noted above are 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, 2023. The Single Audit Report will be available at www.apa.virginia.gov in February 2024.

**Exit Conference and Report Distribution**

We discussed this report with management at an exit conference held on January 31, 2024. Government Auditing Standards require the auditor to perform limited procedures on Education's response to the findings identified in our audit, which is included in the accompanying section titled "Agency Response." Education's response was not subjected to the other auditing procedures applied in the audit and, accordingly, we express no opinion on the response.

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.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

DGS/vks

## FINDINGS SUMMARY

| Finding Title | Status of Corrective Action | First Issued |
|---|---|---|
| Ensure the Correct Award Year is Applied to Federal Reports | Ongoing | 2022 |
| Improve Vulnerability Management Process | Ongoing | 2023 |
| Improve IT Risk Management Program | Ongoing | 2023 |
| Improve Third-Party Service Provider Process | Ongoing | 2023 |

COMMONWEALTH of VIRGINIA

Lisa Coons, Ed.D.
Superintendent of Public Instruction

DEPARTMENT OF EDUCATION
P.O. BOX 2120
RICHMOND, VA 23218-2120

Office: (804) 225-2057
Fax: (804) 371-2099

February 2, 2024

Ms. Staci Henshaw
Auditor of Public Accounts
Post Office Box 1295
Richmond, Virginia 23218-1295

Dear Ms. Henshaw:

I appreciate the opportunity to respond to the findings of the audit completed by the Auditor of Public Accounts of the Virginia Department of Education (VDOE) and Direct Aid to Public Education, for the fiscal year ended June 30, 2023. 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 three matters involving internal control and its operation necessary to bring to management's attention that also represent instances of noncompliance with applicable laws and regulations or other matters that are required to be reported and two issues that are beyond the corrective action of Education's management and require the cooperation of the Virginia Information Technologies Agency (VITA) to address the risks, which are noted in the audit report as "Risk Alerts."

Regarding the finding related to *Improve Vulnerability Management Process*, the VDOE Office of Cybersecurity and Risk Management will continue to work with the VDOE Technology team to help formalize their process for vulnerability patch management. The VDOE Technology team is working on an automated process for opening tickets to help with tracking of patches both internally and externally to the VITA service tower. This should help with the timeliness of vulnerability patch management.

Regarding the finding related to *Improve IT Risk Management Program*, the VDOE Cybersecurity and Risk Management office is in the process of implementing a new Risk Management program. There was a delay in the implementation due to staff turnover and procurement delays. The VDOE Office of Cybersecurity and Risk Management fully understands the importance of maintaining a strong risk program. New policy and procedures will enable the Office of Cybersecurity and Risk Management at VDOE to have a full picture of the risk to our environment.

Regarding the finding related to *Improve Third Party Service Provided Process,* the growth of the VDOE technical footprint has doubled in the past 18 months. VITA's Enterprise Services group and VDOE will be working to establish roles and responsibilities between the agency and VITA needed to maintain Third Party Service providers. There are several parties at VDOE that are involved in the process of maintaining a strong 3rd party risk approach.

VDOE's Office of Cybersecurity and Risk Management will own the ECOS process going forward. With the change VDOE should have a mature process for ECOS and 3rd party Risk Management.

Regarding the *Risk Alert – Unpatched Software*, agency management recognizes that there is a risk associated with software that has not been patched by the Virginia Information Technologies Agency (VITA). This risk will be mitigated now that major VDOE technology systems have been migrated to the cloud and the system freeze has been lifted. Furthermore, VDOE has technical staff dedicated to monitoring the patching, as well as ensuring service tickets to VITA are completed in a timely manner.

Regarding the *Risk Alert – Access to Audit Log Monitoring*, VDOE is working with VITA to implement its new log monitoring tool. The previous product that was offered did not provide the agency a granular view into the VDOE technology environment. If the new solution being offered by VITA does not provide the necessary information, VDOE has purchased and implemented their own solution.

Thank you for the opportunity to provide an agency response to the fiscal year 2023 audit report. The Virginia 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,

Lisa Coons Digitally signed by Lisa Coons
Date: 2024.02.06 16:19:32 -05'00'

Lisa Coons, Ed.D.
Superintendent of Public Instruction

LC/as