STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2024-198
May 2024

ST. JOHNS COUNTY DISTRICT SCHOOL BOARD

PowerSchool Unified Administration^{TM} BusinessPlus and PowerSchool eSchoolPlus Student Information System

Sherrill F. Norman, CPA
Auditor General

Board Members and Superintendent

During the period January 2023 through December 2023, Tim Forson served as Superintendent of the St. Johns County Schools and the following individuals served as School Board Members:

	District No.
Beverly Slough, Chair from 11-14-23, Vice Chair through 11-13-23	1
Anthony Coleman Sr., Vice Chair from 11-14-23	2
Jennifer Collins	3
Kelly Barrera, Chair through 11-13-23	4
Patrick Canan	5

The team leader was Sue Graham, CPA, CISA, and the audit was supervised by Heidi Burns, CPA, CISA.

Please address inquiries regarding this report to Heidi Burns, CPA, CISA, Audit Manager, by e-mail at heidiburns@aud.state.fl.us or by telephone at (850) 412-2926.

This report and other reports prepared by the Auditor General are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General
Claude Pepper Building, Suite G74 · 111 West Madison Street · Tallahassee, FL 32399-1450 · (850) 412-2722

ST. JOHNS COUNTY DISTRICT SCHOOL BOARD

PowerSchool Unified Administration^{TM} BusinessPlus and PowerSchool eSchoolPlus Student Information System

SUMMARY

This operational audit of St. Johns County School District (District) focused on selected information technology (IT) controls applicable to PowerSchool Unified Administration^{TM} BusinessPlus system, the PowerSchool eSchoolPlus Student Information System, and the District's IT infrastructure, and included a follow-up on findings noted in our report No. 2020-053. Our audit disclosed the following:

Finding 1: District security awareness training needs improvement to reduce the risk of compromising District data and IT resources.

Finding 2: District IT security controls related to user authentication and account management need improvement to ensure the confidentiality, integrity, and availability of District data and IT resources. A similar finding related to user authentication was noted in our report No. 2020-053.

BACKGROUND

The St. Johns County School District (District) is part of the State system of public education under the general direction of the Florida Department of Education and is governed by State law and State Board of Education rules. Geographic boundaries of the District correspond with those of St. Johns County. The governing body of the District is the St. Johns County District School Board (Board), which is comprised of five elected members. The appointed Superintendent of Schools is the Executive Officer of the Board. During the 2022-23 fiscal year, the District operated 47 schools, including 44 elementary, K-8, middle, high, virtual, and alternative schools; 1 technical college; 2 juvenile justice programs; sponsored 3 charter schools; and reported 50,414 unweighted full-time equivalent students.

The District uses PowerSchool Unified Administration^{TM} BusinessPlus (BusinessPlus) to process and report financial and human resources information and PowerSchool eSchoolPlus Student Information System (eSchoolPlus) to process and report student information. In addition, the District maintains and manages the information technology infrastructure supporting BusinessPlus and eSchoolPlus, including the network domain, application and database servers, and database management systems.

FINDINGS AND RECOMMENDATIONS

Finding 1: Security Awareness Training

A comprehensive security awareness training program instructing all employees on the importance of preserving the confidentiality, integrity, and availability of data and information technology (IT) resources entrusted to them is a foundational control for security vigilance and preventing and mitigating cybersecurity risks. An effective security awareness program includes identification of the specific knowledge, skills, and abilities needed to support District security and educates all employees about how to interact with data and IT resources in a secure manner.

As part of our audit, we examined District procedures and related records supporting annual employee security awareness and skills training. We found that the District assigned training on July 1, 2023, to all District employees for the 2023-24 school year using vendor-provided modules, including phishing, social engineering, password strength, and reporting suspicious e-mails. The vendor-provided training platform tracked the progress of user completion and automatically sent reminder notifications for completion and, according to District management, employees should have completed the training by the second week of October 2023. However, as of March 26, 2024, 21 percent of the employees had not completed the training and neither Board policies nor District procedures required employees to complete the training or established consequences for those who did not complete the training. In response to our inquiry, District IT management stated that while effort was made by the Chief Information Officer to drive training completion, they did not have enforcement authority to ensure all users completed security awareness training.

Additionally, although the vendor-provided platform had a module addressing the Family Educational Rights and Privacy Act protecting the privacy of student educational records, the module was not included in the assigned training. Consequently, the training did not educate employees about data handling best practices, such as District controls specific to storage and transmission of confidential and sensitive data.

Effective security awareness training programs include data handling best practices and instructions to understand causes of unintentional data exposure and require completion by all employees. The lack of a comprehensive security awareness training program increases the risk that employees may compromise the confidentiality, availability, and integrity of District data and IT resources.

Recommendation: To reduce cybersecurity risks, District management should establish a comprehensive security awareness training program that educates employees about data handling best practices specific to District controls and ensures that all employees are aware of their responsibilities for securing District data and IT resources. In addition, the program should require all employees to complete the training within a specified period and establish consequences for those who do not timely complete the training.

Finding 2: Security Controls - User Authentication and Account Management

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed certain security controls related to user authentication and account management need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the confidentiality of District data and related IT resources. However, we have notified appropriate District management of the two findings in the areas needing improvement. A similar finding related to user authentication was noted in our report No. 2020-053.

Without appropriate security controls related to user authentication and account management, the risk is increased for the confidentiality, integrity, and availability of District data and related IT resources to be compromised.

Recommendation: We recommend that District management improve IT security controls related to user authentication and account management to ensure the confidentiality, integrity, and availability of District data and IT resources.

PRIOR AUDIT FOLLOW-UP

Except as discussed in Finding 2, the District had taken corrective actions for the findings included in our report No. 2020-053.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this information technology (IT) operational audit from October 2023 through March 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected significant IT controls applicable to PowerSchool Unified Administration^{TM} BusinessPlus (BusinessPlus), the PowerSchool eSchoolPlus Student Information System (eSchoolPlus), and District IT infrastructure during the 2023 calendar year and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To determine the effectiveness of selected significant IT controls in achieving management's objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To determine whether management had taken corrective actions for findings included in our report No. 2020-053.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the IT systems included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT systems included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of and evaluating the IT systems and related significant controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, waste, abuse, or inefficiency.

In conducting this audit, we:

- Reviewed applicable laws, rules, and other guidelines to obtain an understanding of District organizational structure and regulatory requirements; reviewed District procedures, interviewed District personnel, and examined District records to obtain an understanding of District operations related to BusinessPlus, eSchoolPlus, and IT infrastructure and to evaluate whether District operations were designed properly and operating effectively.
- Evaluated the sufficiency of District controls; observed, documented, and tested key processes, procedures, and controls related to BusinessPlus and eSchoolPlus and the District IT infrastructure, including authentication, backup and recovery, configuration of systems, logical controls, and inventory and vulnerability management.
- Examined selected security settings related to the District network infrastructure, externally facing applications, remote access systems, and other critical servers and devices to determine whether authentication controls were configured and enforced in accordance with IT best practices, including the use of multi-factor authentication.
- Evaluated the effectiveness of District logical access controls assigned to the District network and servers supporting BusinessPlus and eSchoolPlus, including the periodic evaluation of assigned accounts.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges as of September 21, 2023, within the four default network administrator system groups for the District network domain.
- Examined and evaluated the appropriateness of administrative access privileges as of September 21, 2023, to the 7 servers supporting BusinessPlus and 19 servers supporting eSchoolPlus.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges as of October 2, 2023, for the two high-risk network devices.
- Examined and evaluated selected District patch management controls for operating systems and network devices to ensure that secure configurations are maintained. Specifically, we examined and evaluated the patch management controls for:
  - The 26 servers supporting BusinessPlus and eSchoolPlus as of September 21, 2023.
  - The 2 high-risk network devices as of October 3, 2023.

- Evaluated the effectiveness of logical controls assigned within eSchoolPlus.
- Examined and evaluated the appropriateness of access privileges as of September 21, 2023, granted to the 12 critical roles and the security administration function within eSchoolPlus for 82 employees.
- Examined and evaluated as of September 21, 2023, 74 database principals (users, groups, and roles) assigned to the database supporting BusinessPlus and 96 database principals assigned to the database supporting eSchoolPlus.
- Evaluated District controls in place for the use of impersonation privileges.
- Evaluated the effectiveness of the District's logging and monitoring controls, including security events and actions performed by privileged users for the servers and databases supporting BusinessPlus and eSchoolPlus.
- Evaluated District procedures and examined selected records to determine the adequacy of District procedures for maintaining a software asset inventory and ensuring only authorized software is installed on the network.
- Evaluated the effectiveness of District configuration management controls, including establishing and maintaining secure configurations; disabling insecure protocols; implementing firewalls or port filtering to protect network resources; and timely applying software updates and managing device end-of-life.
- Evaluated District procedures and examined selected scan reports and policies to evaluate the adequacy of District vulnerability management controls related to the IT infrastructure, including vulnerability assessment and remediation, malicious software identification, and malware defense.
- Evaluated District procedures and examined selected backup reports to determine the adequacy of the District data recovery procedures to restore District IT assets to a pre-incident trusted state.
- Evaluated the effectiveness of the District security awareness training program.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

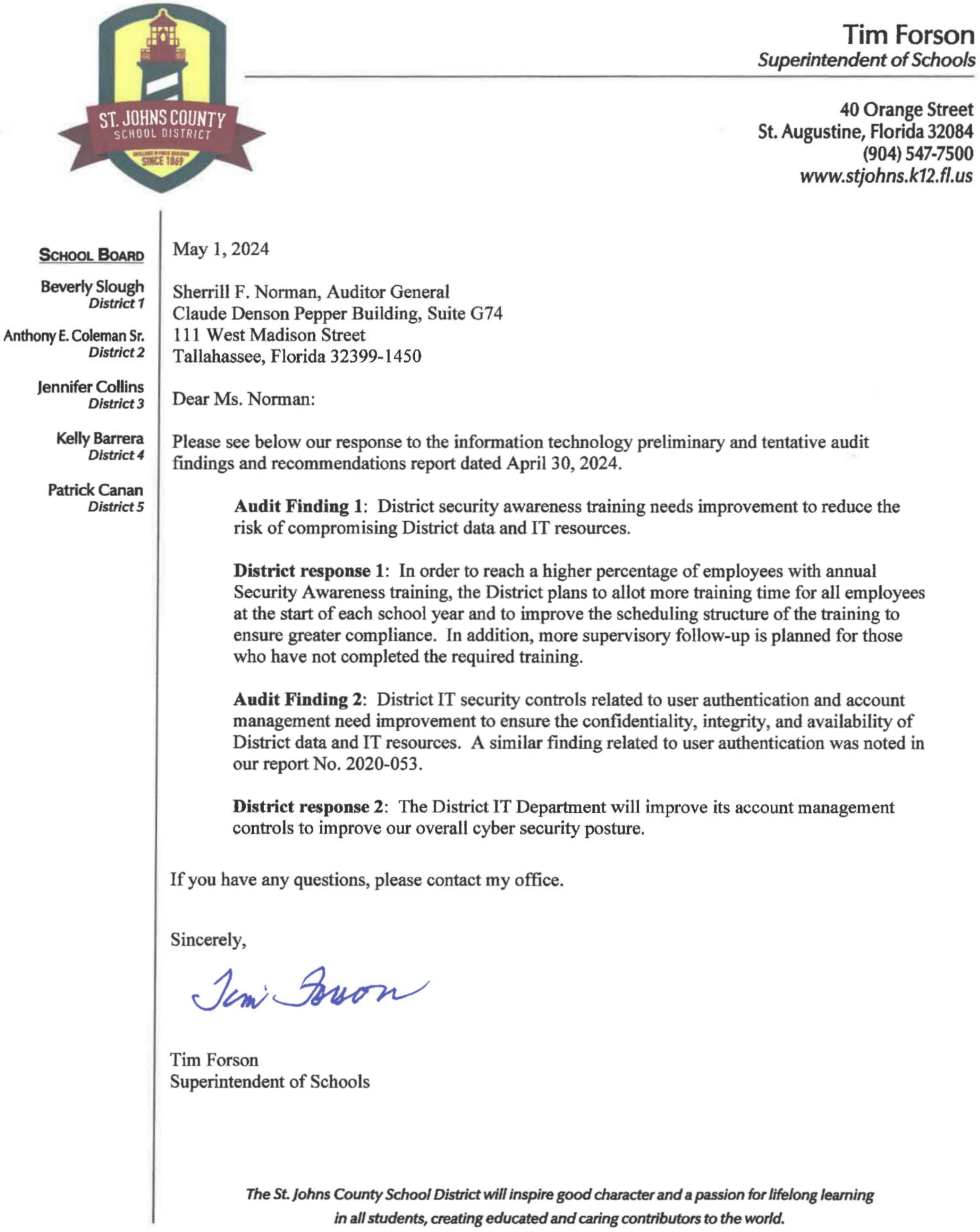
AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

Sherrill F. Norman

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE



ST. JOHNS COUNTY
SCHOOL DISTRICT
SINCE 1869

Tim Forson
Superintendent of Schools

40 Orange Street
St. Augustine, Florida 32084
(904) 547-7500
www.stjohns.k12.fl.us

SCHOOL BOARD

Beverly Slough
District 1

Anthony E. Coleman Sr.
District 2

Jennifer Collins
District 3

Kelly Barrera
District 4

Patrick Canan
District 5

May 1, 2024

Sherrill F. Norman, Auditor General
Claude Denson Pepper Building, Suite G74
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Please see below our response to the information technology preliminary and tentative audit findings and recommendations report dated April 30, 2024.

> **Audit Finding 1**: District security awareness training needs improvement to reduce the risk of compromising District data and IT resources.
>
> **District response 1**: In order to reach a higher percentage of employees with annual Security Awareness training, the District plans to allot more training time for all employees at the start of each school year and to improve the scheduling structure of the training to ensure greater compliance. In addition, more supervisory follow-up is planned for those who have not completed the required training.
>
> **Audit Finding 2**: District IT security controls related to user authentication and account management need improvement to ensure the confidentiality, integrity, and availability of District data and IT resources. A similar finding related to user authentication was noted in our report No. 2020-053.
>
> **District response 2**: The District IT Department will improve its account management controls to improve our overall cyber security posture.

If you have any questions, please contact my office.

Sincerely,

Tim Forson

Tim Forson
Superintendent of Schools

The St. Johns County School District will inspire good character and a passion for lifelong learning in all students, creating educated and caring contributors to the world.