STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2020-156
March 2020

LEON COUNTY DISTRICT SCHOOL BOARD

Focus Student Information System
and Prior Audit Follow-up

Sherrill F. Norman, CPA
Auditor General

Board Members and Superintendent

During the period, June 2019 through November 2019, Rocky Hanna served as Superintendent of the Leon County School Board and the following individuals served as School Board Members.

	District No.
Alva Striplin	1
Rosanne Wood, Chair through 11-18-19	2
Darryl Jones	3
DeeDee Rasmussen, Chair from 11-19-19, Vice Chair through 11-18-19	4
Georgia “Joy” Bowen, Vice Chair from 11-19-19	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

LEON COUNTY DISTRICT SCHOOL BOARD

Focus Student Information System and Prior Audit Follow-up

SUMMARY

This operational audit of Leon County District School Board (District) focused on evaluating selected information technology (IT) controls applicable to the Focus Student Information System (Focus) used for recording, processing, and reporting student-related information and the supporting infrastructure and included a follow-up on findings applicable to the District's Skyward school business suite software included in our report No. 2018-027. As summarized below, our audit disclosed areas in which improvements in the District's controls and operational processes are needed.

Finding 1: Some District employees' access privileges within Focus were unnecessary for the employees' assigned job responsibilities.

Finding 2: District controls related to mobile device management need improvement.

Finding 3: District IT security controls related to user authentication, account management, monitoring, and vulnerability management need improvement to ensure the confidentiality, integrity, and availability of District data and IT resources.

BACKGROUND

The Leon County School District (District) is part of the State system of public education under the general direction of the Florida Department of Education. The governing body of the District is the Leon County District School Board (Board), which is comprised of five elected members. The elected Superintendent of Schools is the executive officer of the Board. During the 2018-19 fiscal year, the District had 54 centers and schools other than charter schools, 4 charter schools, and reported 40,746 unweighted full-time equivalent students.

The District uses Skyward to process and report its finance and human resources (HR) transactions and the Focus Student Information System (Focus) for the recording, processing, and reporting of student-related transactions. In addition, the District maintains and manages the network domains supporting Skyward and Focus.

FINDINGS AND RECOMMENDATIONS

Finding 1: Appropriateness of Access Privileges

Access controls are intended to protect data and information technology (IT) resources from unauthorized disclosure, modification, or destruction. Effective access controls include measures that promote an appropriate separation of duties and restrict the access privileges granted to employees to only those necessary for assigned responsibilities or functions. Such access controls are essential to protect the confidentiality, integrity, and availability of data and IT resources. Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure.

The access privileges within Focus are controlled by assigning profiles to users. Permissions to access certain modules and view or edit specific screens and fields are defined to each profile. We reviewed the profiles assigned to 35 of 3,125 users to determine the appropriateness of assigned access to student attendance, discipline, grades, and health information. Our review disclosed that the system administrator profile assigned to the Director of Applications, two System Programs Managers, and one Computer Systems Analyst allowed unnecessary update access to all functions within Focus, including transaction origination, correction, and changes to student data.

In response to our audit inquiry, District management stated that the profile had been assigned to facilitate data changes needed since the implementation of Focus in August 2018 and indicated that it would be removed from one System Programs Manager and the Computer System Analyst. Although the system administrator profile must be assigned to one user account in Focus for the District, each of these employees' day-to-day responsibilities did not require complete update access privileges to Focus and such privileges are contrary to an appropriate separation of end-user and technical support functions.

Appropriately restricted access privileges help protect District data and IT resources from unauthorized modification, loss, or disclosure.

Recommendation: We recommend that District management ensure that the system administrator profile granted within Focus is necessary and appropriate for the employee's assigned responsibilities.

Finding 2: Mobile Device Management

Effective mobile device management includes establishing policies and procedures related to how the entity will manage the configuration and security of each mobile device (cellular telephone, smart phone, laptop, or tablet), whether entity or employee-owned, before allowing the device to access entity data and IT resources. Well-designed policies and procedures include defined security requirements for mobile devices pertaining to device encryption, current standard configuration, patching, anti-virus protection, and passcode protection. In addition, established policies and procedures should define the responsibilities of the entity and the user when mobile devices are used to connect to an entity's network and IT resources. The effective implementation of such policies and procedures requires an inventory of all mobile devices authorized to connect to an entity's network environment and the ability to systematically enforce defined security requirements.

Board policies[1] allow employee access to confidential and sensitive data on the District's network using personally owned mobile devices. However, although the District had established security requirements, such as use of a passcode, device encryption for stored confidential information, and current virus protection for mobile devices, and device loss reporting responsibilities, the District had not established minimum operating system requirements or required acknowledgement from employees of the requirements. In addition, the District did not maintain an inventory of the personally owned mobile devices authorized to connect to the District's network environment or establish the ability to

[1] Board Policy 7530.02, *District Personnel's Use of Wireless Communication Devices*, and Policy 7543, *Utilization of the District's Website and Remote Access to the District's Network*.

systematically enforce security requirements for these devices thereby limiting the prevention and detection of unauthorized mobile devices' access to the network.

Effective mobile device management through established and enforceable security requirements and user responsibilities help ensure the confidentiality, integrity, and availability of District data and IT resources.

Recommendation: We recommend that District management establish minimum operating system requirements for personally owned mobile devices connecting to the District's network and establish an agreement for the use of personally owned mobile devices, including system requirements and device loss reporting responsibilities. We also recommend that District management maintain a complete inventory of personally owned mobile devices authorized to connect to the District's network and systematically enforce established security requirements for those devices.

Finding 3: Security Controls – User Authentication, Account Management, Monitoring, and Vulnerability Management

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to user authentication, account management, monitoring, and vulnerability 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 specific issues.

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

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

PRIOR AUDIT FOLLOW-UP

The District had taken corrective actions for the findings included in our report No. 2018-027.

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 IT operational audit from June 2019 through November 2019 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 IT controls applicable to the Focus Student Information System (Focus) during the period June 2019 through November 2019 and to follow up on deficiencies disclosed in audit report No. 2018-027. The overall objectives of the audit were:

- To evaluate the effectiveness of selected IT controls in achieving management's control 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 has corrected, or is in the process of correcting, all deficiencies disclosed in audit report No. 2018-027.
- 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 and controls 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 and controls 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 the IT systems and 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, abuse, or inefficiency.

In conducting this audit, we:

- Interviewed District staff and reviewed District records to obtain an understanding of District operations for Focus and the supporting network, including authentication, logical controls, and logging and monitoring of the network, and vulnerability management; Focus application logical controls, change management, and logging and monitoring; data and business process flows within Focus; mobile device management for personally owned mobile devices connecting to the District's network; and security management.

- Evaluated the effectiveness of logical access controls, including the periodic reviews of access for the network domains and the Focus application.
- Examined and evaluated the appropriateness of administrative privileges for the District's network domains and child domains as of June 19, 2019 and August 28, 2019.
- Evaluated the effectiveness of logical controls assigned within Focus, including periodic reviews of access privileges.
- Examined and evaluated the appropriateness of access privileges, as of October 9, 2019, granted within Focus for 35 employees.
- Evaluated user authentication controls related to the District IT Infrastructure supporting Focus access.
- Evaluated the effectiveness of the District's change management controls related to the authorization, testing, and approval of Focus data changes.
- Evaluated the effectiveness of the District's vulnerability management (logging, monitoring, and remediation) for the network and critical network infrastructure components supporting Focus.
- Evaluated the effectiveness of the District's logging and monitoring controls related to student information within Focus.
- Evaluated the effectiveness of controls over administrative access to computers on the District's network.
- Evaluated the effectiveness of the District's mobile device security plan, including security and configuration requirements and District- and user-defined responsibilities.
- Evaluated whether management had corrected, or was in the process of correcting, the deficiencies noted in audit report No. 2018-027, which related to user authentication, logging, and security management.
- 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***.

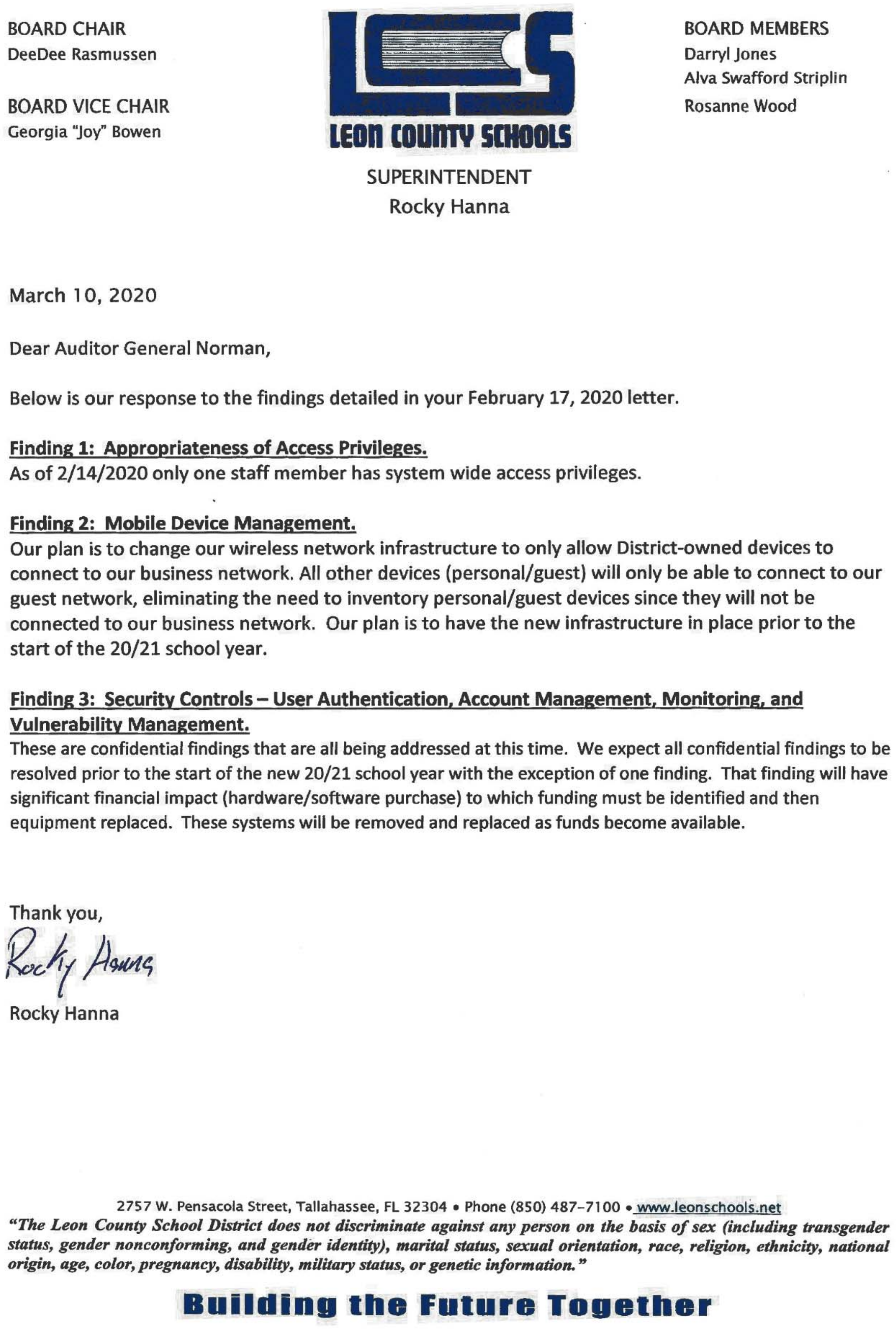
AUTHORITY

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



BOARD CHAIR
DeeDee Rasmussen

BOARD VICE CHAIR
Georgia "Joy" Bowen

LEON COUNTY SCHOOLS

SUPERINTENDENT
Rocky Hanna

BOARD MEMBERS
Darryl Jones
Alva Swafford Striplin
Rosanne Wood

March 10, 2020

Dear Auditor General Norman,

Below is our response to the findings detailed in your February 17, 2020 letter.

Finding 1: Appropriateness of Access Privileges.
As of 2/14/2020 only one staff member has system wide access privileges.

Finding 2: Mobile Device Management.
Our plan is to change our wireless network infrastructure to only allow District-owned devices to connect to our business network. All other devices (personal/guest) will only be able to connect to our guest network, eliminating the need to inventory personal/guest devices since they will not be connected to our business network. Our plan is to have the new infrastructure in place prior to the start of the 20/21 school year.

Finding 3: Security Controls – User Authentication, Account Management, Monitoring, and Vulnerability Management.
These are confidential findings that are all being addressed at this time. We expect all confidential findings to be resolved prior to the start of the new 20/21 school year with the exception of one finding. That finding will have significant financial impact (hardware/software purchase) to which funding must be identified and then equipment replaced. These systems will be removed and replaced as funds become available.

Thank you,

Rocky Hanna

Rocky Hanna

2757 W. Pensacola Street, Tallahassee, FL 32304 • Phone (850) 487-7100 • www.leonschools.net

"The Leon County School District does not discriminate against any person on the basis of sex (including transgender status, gender nonconforming, and gender identity), marital status, sexual orientation, race, religion, ethnicity, national origin, age, color, pregnancy, disability, military status, or genetic information."

Building the Future Together