STATE OF FLORIDA AUDITOR GENERAL

Operational Audit

Report No. 2021-015
September 2020

INDIAN RIVER COUNTY
DISTRICT SCHOOL BOARD

Sherrill F. Norman, CPA
Auditor General

Board Members and Superintendent

During the 2018-19 fiscal year, Dr. Susan Moxley served as Superintendent of the Indian River County Schools from 5-25-19, Dr. Mark J. Rendell served as Superintendent before that date, and the following individuals served as School Board Members:

	District No.
Dr. Mara Schiff from 11-20-18	1
Shawn Frost, Chair through 11-19-18	1
Jacqueline Rosario from 11-20-18	2
Dale Simchick through 11-19-18	2
Laura Zorc, Chair from 11-20-18	3
Teri L. Barenborg from 11-20-18	4
Charles Searcy, Vice Chair through 11-19-18	4
Tiffany M. Justice, Vice Chair from 11-20-18	5

The team leader was Bevohn Dougall, CPA, and the audit was supervised by Tim L. Tucker, CPA.

Please address inquiries regarding this report to Edward A. Waller, CPA, Audit Manager, by e-mail at tedwaller@aud.state.fl.us or by telephone at (850) 412-2887.

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

INDIAN RIVER COUNTY DISTRICT SCHOOL BOARD

SUMMARY

This operational audit of the Indian River County School District (District) focused on selected District processes and administrative activities and included a follow-up on findings noted in our report No. 2017-095. Our audit disclosed the following:

Finding 1: District school safety policies and procedures need improvement.

Finding 2: District controls over payments for school resource officers could be enhanced.

Finding 3: The District did not always provide financial reports monthly to the Board. Such reports provide the Board with information needed for policy decisions.

Finding 4: Some unnecessary information technology (IT) user access privileges existed that increased the risk that unauthorized disclosure of sensitive personal information of students may occur.

Finding 5: Some inappropriate or unnecessary IT access privileges were granted to District employees. A similar finding was noted in our report No. 2017-095.

Finding 6: The District had not established a comprehensive IT risk assessment.

BACKGROUND

The Indian River 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 Indian River County. The governing body of the District is the Indian River County District School Board (Board), which is composed of five elected members. The appointed Superintendent of Schools is the Executive Officer of the Board. During the 2018-19 fiscal year, the District operated 21 elementary, middle, and high schools and 2 specialized schools; sponsored five charter schools; and reported 17,418 unweighted full-time equivalent students.

FINDINGS AND RECOMMENDATION

Finding 1: School Safety

State law[1] requires the Board to formulate and prescribe policies and procedures for emergency drills associated with active shooter and hostage situations and the drills must be conducted at least as often as other emergency drills. Pursuant to the Florida Fire Prevention Code (Fire Code)[2] and Board policies,[3] fire emergency drills must generally be conducted every month a facility is in session. In May 2019, the

[1] Section 1006.07(4), Florida Statutes, as amended by Chapter 2018-3, Laws of Florida (The Marjory Stoneman Douglas High School Public Safety Act).

[2] Section 20.2.4.2.3 of the Florida Fire Prevention Code, 6th Edition (2017).

[3] Board Policy 8420, *Emergency Evacuation of Schools*.

Florida Department of Education (FDOE) issued guidance to address the most frequently asked questions and reinforce the Legislature's intent regarding the State law school safety provisions, including the frequency of school safety drills.

Board policies[4] require the Superintendent to develop a school safety plan to provide for the safety and welfare of the students and staff, as well as a system of emergency preparedness and accompanying procedures. District emergency procedures[5] require that both fire and critical incident drills be performed and that schools maintain and complete a drill log and an after-action report to document the date and type of drill conducted and problems encountered during the drills and recommendations for improvement. According to District personnel, critical incident drills include active shooter and hostage situation drills. However, the District had not established verification procedures to ensure that the emergency drills were conducted and documented for each school.

To determine whether, during the 2018-19 fiscal year, the District and District-sponsored charter schools conducted the required emergency drills (10 active shooter and hostage situation emergency drills and 10 fire emergency drills) at each of the 21 District elementary, middle, and high schools and 5 charter schools, we requested for examination support for all 520 (260 active shooter and hostage situation and 260 fire) emergency drills. However, District records were not available to demonstrate the conduct of 131 (50 percent) of the 260 active shooter and hostage situation emergency drills and 13 (5 percent) of the 260 fire emergency drills.[6]

In response to our inquiries, District personnel indicated that they were unaware that both drills were required monthly until FDOE issued the May 2019 guidance. Notwithstanding, State law and the Fire Code established the frequency of the drills for the entire 2018-19 school year and the FDOE guidance reinforced existing school safety requirements. Absent effective procedures to ensure that all required active shooter and hostage situation and fire emergency drills are timely conducted and documented, the District cannot demonstrate compliance with State law and the Fire Code or that appropriate measures have been taken to promote student and staff safety.

Recommendation: The District should enhance procedures to demonstrate compliance with the State school safety laws. Such enhancements should include documented verifications that, for each month school is in session, District and charter schools conduct active shooter and hostage situation and fire emergency drills.

Finding 2: School Resource Officer Services

Effective contract management requires and ensures that records are maintained to evidence satisfactory receipt of contracted services by personnel with direct knowledge of the services received prior to payment. For the period July 1, 2018, through June 30, 2019, the District incurred expenditures totaling $19.1 million for contracted services.

[4] Board Policy 8405, *School Safety and Security*.

[5] *Indian River Schools, Emergency Management Plan Manual*.

[6] Of the 131 unsupported active shooter and hostage situation emergency drills, 113 drills related to the 21 District schools and 18 related to the 5 charter schools. Of the 13 unsupported fire emergency drills, 9 drills related to the 21 District schools and 4 related to the 5 charter schools.

As part of our procedures, we examined District records supporting 28 selected payments totaling $3 million related to 24 contracts. While District records indicated that the District designed and implemented internal controls that generally ensure payments are consistent with contract terms and provisions, we identified certain control deficiencies for contracting and monitoring payments, totaling $1 million, related to 3 school resource officer (SRO) contracts. We expanded our procedures to evaluate District records supporting all payments associated with SRO contracts for the 2018-19 fiscal year.

We found that the Board approved contracts totaling $1 million for the 2018-19 fiscal year with 3 law enforcement agencies for SRO services at the District's 21 schools. The contracts provided for 50 percent of the costs of two full-time supervisors, 20 deputies, and 4 policemen assigned to the District and that the services would be equally billed on semi-annual invoices provided by each law enforcement agency. However, District procedures had not been established to require and ensure that school personnel with direct knowledge of the services verified and documented satisfactory receipt of the services.

In response to our inquiry, District personnel indicated that they rely upon the law enforcement attendance procedures to ensure that the SROs provide services in accordance with the contract. Notwithstanding, District reliance on the procedures of the law enforcement agencies provides limited assurance that the services were received as expected. Absent established procedures that require verification and documentation of the satisfactory receipt of contracted services by personnel with direct knowledge of the services prior to payment, there is an increased risk that the District may overpay for such services, the services may not be received consistent with Board expectations, and any overpayments that occur may not be timely detected or recovered.

Recommendation: The District should enhance procedures to ensure that, prior to payment, school personnel with direct knowledge of the SRO verify and document satisfactory receipt of the services.

Finding 3: Monthly Financial Reports

State Board of Education (SBE) rules[7] require that the Superintendent, at least monthly, submit financial statements (reports) for use and consideration by the Board. Our review of District records for the 2018-19 fiscal year disclosed that, contrary to SBE rules, the Superintendent only submitted financial reports during 6 months of the 2018-19 fiscal year, reducing the effectiveness of Board's financial monitoring procedures.

In response to our inquiry, District personnel indicated that monthly reporting was not always performed because of staffing changes and attention given to the new enterprise resource planning (ERP) system implemented in January 2019. District personnel also provided records evidencing that the financial information for 1 of the omitted reports was combined with information for another month and reported to the Board. Subsequent to our inquiry, District personnel submitted the other 5 omitted monthly reports to the Board in September 2019.

[7] SBE Rule 6A-1.008, Florida Administrative Code.

While, as of June 30, 2019, the Board reported no budgetary over expenditures, monthly financial reports help the Board make effective and efficient management decisions and avoid financial mismanagement.

Recommendation: The District should continue efforts to ensure that financial reports are provided monthly to the Board.

Finding 4: Information Technology User Access Privileges to Sensitive Personal Student Information

The Legislature has recognized in State law[8] that social security numbers (SSNs) can be used to acquire sensitive personal information, the release of which could result in fraud against individuals or cause other financial or personal harm. Therefore, public entities are required to provide extra care in maintaining the confidential status of such information. Effective controls restrict employees from accessing information unnecessary for their assigned job responsibilities and provide for documented, periodic evaluations of information technology (IT) user access privileges to help prevent employees from accessing sensitive personal information of students inconsistent with their responsibilities.

Pursuant to State law,[9] the District identified each student using a Florida education identification number assigned by the FDOE. However, student SSNs are included in the student records maintained within the District management information system (MIS). Student SSNs are maintained in the District MIS to, for example, register newly enrolled students and transmit that information to the FDOE through a secure-file procedure and provide student transcripts to colleges, universities, and potential employers based on student-authorized requests. Board policies[10] identify student SSNs as confidential data and provide that access to confidential data shall be limited to authorized District officials or agents with a legitimate academic or business interest.

As of November 2019, the District MIS contained the sensitive personal information for 109,246 students, including 19,220 current and 90,026 former District students, and 212 District employees had IT user access privileges to that information. As part of our audit procedures, we inquired of District personnel and examined District records supporting access privileges for all employees who had access to sensitive personal information of students. According to District personnel, periodic evaluations of access were not performed and we found that 70 employees, including school principals, assistant principals, and guidance counselors, did not require access to sensitive personal information of students perform their job responsibilities.

District personnel also indicated that the MIS did not include a mechanism to differentiate the access privileges to current student information from the access privileges to former student information and employees with access privileges to both former and current student information did not always have a demonstrated need for that access. The existence of unnecessary IT access privileges increases the risk of unauthorized disclosure of sensitive personal information of students and the possibility that such information may be used in fraud against District students or others.

[8] Section 119.071(5)(a), Florida Statutes.

[9] Section 1008.386, Florida Statutes.

[10] Board Policy 8330, *Student Records.*

Recommendation: To ensure that sensitive personal information of students is properly safeguarded, the District should document periodic evaluations of the necessity for IT user access privileges to such information and timely remove any inappropriate or unnecessary access privileges detected. If an employee only requires occasional access to the information, the privileges should be granted only for the time needed. In addition, the District should take appropriate action, such as upgrading the District MIS, to differentiate IT user access privileges to current student information from access privileges to former student information.

Finding 5: Information Technology User Access Privileges to Human Resource and Payroll Applications

Access controls are intended to protect data and IT resources from unauthorized disclosure, modification, or destruction. Effective access controls provide employees access to IT resources based on a demonstrated need to view, change, or delete data and restrict employees from performing incompatible functions or functions outside of their areas of responsibilities. Periodic evaluations of assigned IT access privileges are necessary to ensure that employees can only access those IT resources that are necessary to perform their assigned job responsibilities. In January 2019, the District implemented a new finance, payroll, and human resource (HR) ERP system.

District personnel indicated that, due to infrequent employee responsibility changes, user profiles are not periodically reviewed and updated. Consequently, the District had not established procedures to periodically review detailed access reports to identify the propriety of access privileges for each employee.

As part of our audit, we obtained a listing of 238 employees with IT access privileges to the District's business application, including the finance and HR modules and selected the access privileges of 27 employees to evaluate whether the privileges were consistent with the employees' job responsibilities. We found that the access privileges and job responsibilities were incompatible for 9 of the employees. Specifically:

- The District Payroll Manager (Manager) had privileges that were incompatible with her duties. For example, the Manager could update the HR module by creating an employee, adjusting salary records, and updating employee address and bank information, which are actions appropriate only for HR Department personnel.
- 8 HR Department employees had the ability to create, update, and edit employee direct deposit information. These access privileges were unnecessary for the employees' assigned job duties and contrary to an appropriate separation of duties. Subsequent to our inquiries, in December 2019 the District removed this access for these employees.

While District controls (e.g., independent review and verification of District records supporting payroll changes and budgetary monitoring controls) mitigate some of the risks associated with the business application access control deficiencies, the existence of incompatible duties and the absence of periodic evaluations of IT access privileges increase the risk that unauthorized disclosure, modification, or destruction of District data and IT resources may occur and not be timely detected. A similar finding was noted in our report No. 2017-095.

Recommendation: The District should establish and implement periodic IT access privilege evaluations and timely remove any inappropriate or unnecessary access privileges detected. In

addition, the District should remove the Payroll Manager's IT access privileges that are incompatible with her duties.

Follow-Up to Management's Response:

Management's response indicates that "in order to ensure accurate and timely processing of all payroll cycles [the District] granted the District's payroll manager emergency access to correct salary calculation, supplements, etc." Management also indicated that the District understands the exposure and views this as an acceptable risk. Notwithstanding, such access is incompatible with the payroll manager's duties and is only somewhat mitigated by the District's compensating controls; therefore, there is an increased risk for unauthorized disclosure, modification, or destruction of District data and IT resources without timely detection. As such, our recommendation stands as presented.

Finding 6: Information Technology Risk Assessment

Management of IT risks is a key part of enterprise IT governance. Incorporating an enterprise perspective into day-to-day governance helps an entity understand security risk exposures and determine whether controls are appropriate and adequate to secure IT resources from unauthorized disclosure, modification, or destruction. IT risk assessments, including the identification of associated risks, the evaluation of the likelihood of threats resulting from those risks, and the severity of threat impact on enterprise operations, help management make decisions regarding the establishment of cost-effective measures necessary to mitigate significant risks and, where appropriate, to formally accept residual risks.

Although District personnel indicated that they had considered external and internal risks, a comprehensive IT risk assessment had not been established due to staff changes and implementation of the new ERP system. A properly completed comprehensive IT risk assessment considers network vulnerabilities and associated threats at the Districtwide, system, and application levels. Such assessments identify and document vulnerabilities, threats, and risks posed by both internal and external sources and provides a basis for the establishment of appropriate procedures and controls to mitigate risks determined to be significant.

Absent a comprehensive IT risk assessment, the District has limited assurance that all threats and vulnerabilities have been identified, significant risks have been adequately addressed, and appropriate decisions have been made regarding which risks to accept and which risks to mitigate through establishment of appropriate procedures and controls.

Recommendation: The District should establish a comprehensive IT risk assessment to provide a basis for managing significant risks associated with IT operations.

PRIOR AUDIT FOLLOW-UP

The District had taken corrective actions for findings included in our report No. 2017-095, except that Finding 5 was also noted in that report as Finding 6.

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 operational audit from April 2019 to April 2020 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 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.

The objectives of this operational audit were to:

- Evaluate management's performance in establishing and maintaining internal controls, including controls designed to prevent and detect fraud, waste, and abuse, and in administering assigned responsibilities in accordance with applicable laws, rules, regulations, contracts, grant agreements, and other guidelines.
- Examine internal controls designed and placed in operation to promote and encourage the achievement of management's control objectives in the categories of compliance, economic and efficient operations, reliability of records and reports, and safeguarding of assets, and identify weaknesses in those controls.
- Determine whether management had taken corrective actions for findings included in our report No. 2017-095.
- 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 those programs, activities, or functions included within the scope of the audit, weaknesses in management's internal controls, instances of noncompliance with applicable laws, rules, regulations, contracts, grant agreements, and other guidelines; 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 transactions, legal compliance matters, records, and controls considered.

As described in more detail below, for those programs, activities, and functions included within the scope of our 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 our audit; obtaining an understanding of the program, activity, or function; 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 our audit findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our audit included transactions, as well as events and conditions, occurring during the 2018-19 fiscal year audit period, and selected District actions taken prior and subsequent thereto. Unless otherwise indicated in this report, these records and transactions 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 management, staff, and vendors, and as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, waste, abuse, or inefficiency.

In conducting our audit, we:

- Reviewed District information technology (IT) policies and procedures to determine whether the policies and procedures addressed certain important IT control functions, such as security, systems development and maintenance, network configuration management, system backups, and disaster recovery.
- Evaluated District procedures for maintaining and reviewing employee access to IT data and resources. We examined selected access privileges to the District's new enterprise resource planning (ERP) system finance and payroll and human resources (HR) applications to determine the appropriateness and necessity of the access based on employees' job duties and user account functions and whether the access prevented the performance of incompatible duties. We also examined the administrator account access privileges granted and procedures for oversight of administrative accounts for the network and applications to determine whether these accounts had been appropriately assigned and managed. Specifically, from the population of 238 employee accounts, we requested for examination District records supporting the:
    - Critical finance functions for 17 selected finance department employee accounts to determine the appropriateness and necessity of the access privileges based on the employee's job duties.
    - Critical HR functions for 10 HR department employee accounts to determine the appropriateness and necessity of the access privileges based on the employee's job duties.
- Reviewed District procedures to prohibit former employee access to electronic data files. We also reviewed selected user access privileges for 6 of the 283 employees who separated from District employment during the audit period to determine whether the access privileges had been timely deactivated.
- Determined whether a comprehensive IT disaster recovery plan was in place, designed properly, operating effectively, and had been recently tested.
- Determined whether a comprehensive IT risk assessment had been established to substantiate the District's risk management and assessment processes and security controls intended to protect the confidentiality, integrity, and availability of data and IT resources.
- Evaluated the District data center's physical access controls to determine whether vulnerabilities existed.
- Determined whether a fire suppression system had been installed in the District's data center.
- Examined Board meeting minutes and District records for the audit period to determine whether Board approval was obtained for policies and procedures and the records evidenced Board compliance with Sunshine Law requirements (i.e., proper notice of meetings, meetings readily accessible to the public, and properly maintained meeting minutes).

- Analyzed the District's General Fund total unassigned and assigned fund balances at June 30, 2019, to determine whether the total was less than 3 percent of the fund's revenues, as specified in Section 1011.051, Florida Statutes. We also performed analytical procedures to evaluate the District's ability to make future debt service payments.
- Based on discussions with District personnel, review of District procedures, and examination of District records evaluated controls over cash collections for the District's extended day program (EDP). From the population of 13 schools offering EDP with collections totaling $1.2 million for the audit period, we examined District records supporting 30 selected daily deposits totaling $37,542 at 6 schools to determine whether recordkeeping and cash collection duties were separated, transfer documents were maintained, and fees were properly assessed, agreed to attendance records, and were timely deposited.
- From the population of expenditures totaling $12.1 million and transfers totaling $17.8 million during the audit period from nonvoted capital outlay tax levy proceeds, Public Education Capital Outlay funds, and other restricted capital project funds, examined documentation supporting selected expenditures and transfers totaling $11 million and $4.5 million, respectively, to determine District compliance with the restrictions imposed on the use of these resources, including Section 1011.71(2)(e), Florida Statutes.
- From the population of $1.4 million total workforce education program funds expenditures for the audit period, selected 15 expenditures totaling $564,614 and examined supporting documentation to determine whether the District used the funds for authorized purposes (i.e., not used to support K-12 programs or District K-12 administrative costs).
- From the population of 40 industry certifications eligible for the 2018-19 fiscal year performance funding, examined 30 selected certifications to determine whether the District maintained documentation for student attainment of the industry certifications.
- From the population of 50,877 contact hours for 233 adult general education instructional students during the audit period, examined District records supporting 8,347 reported contact hours for 40 selected students to determine whether the District reported the instructional contact hours in accordance with State Board of Education (SBE) Rule 6A 10.0381, Florida Administrative Code.
- Evaluated District procedures for protecting the sensitive personal information of students, including social security numbers. Specifically, we examined the access privileges of the 212 employees who had access to sensitive personal student information to evaluate the appropriateness and necessity of the access privileges based on the employee's assigned job responsibilities.
- Examined District records for the audit period to determine whether District procedures for preparing the budget were sufficient to ensure that all potential expenditures were budgeted.
- For the audit period, examined District budgets and budget amendments to determine whether they were prepared and adopted in accordance with State law and SBE rules.
- Examined financial reports and analyses presented to the Board and applicable Board minutes during the audit period to determine whether the Board monitored financial results and related budget estimates.
- Evaluated Board policies and District procedures for payments of accumulated annual and sick leave (terminal leave pay) to determine compliance with State law and Board policies. From the population of 228 former employees paid $427,181 for terminal leave during the audit period, we examined District records for 10 selected former employees paid terminal leave pay totaling $186,968 to determine whether the terminal leave pay was calculated in compliance with Sections 1012.61 and 1012.65, Florida Statutes, and Board policies.

- Evaluated severance pay provisions in 5 employee contracts including Superintendent's contract to determine whether these severance pay provisions complied with Section 215.425(4), Florida Statutes.
- From the compensation payments totaling $119.7 million to 2,396 employees during the audit period, examined District records supporting compensation payments totaling $52,362 to 30 selected employees to determine the accuracy of the rate of pay and whether supervisory personnel reviewed and approved employee reports of time worked.
- Examined District records supporting the eligibility of:
  - 30 selected District recipients of the Florida Best and Brightest Teacher Scholarship Program awards from the population of 871 District teachers who received scholarships awards totaling $1.4 million during the audit period.
  - 128 selected charter school recipients of the awards from the population of 143 charter school teachers who received scholarships awards totaling $296,792 during the audit period.
- Evaluated the District's procedures to implement the Florida Best and Brightest Principal Scholarship Program pursuant to Section 1012.732, Florida Statutes. We also examined District records to determine whether the District submitted to the FDOE accurate information about the number of classroom teachers and the list of principals, as required by Section 1012.731(4), Florida Statutes, and whether the District timely awarded the correct amount to each eligible principal.
- Evaluated District policies and procedures for ethical conduct for instructional personnel and school administrators, including reporting responsibilities of employee misconduct which affects the health, safety, or welfare of a student, to determine compliance with Section 1001.42(6), Florida Statutes.
- Examined documentation supporting the four payments totaling $505,381 during the audit period for the new ERP system to determine whether the District evaluated the effectiveness and suitability of the system prior to purchase, and deliverables met the contract terms and conditions.
- Examined District records to determine whether the Board had adopted appropriate school safety policies and the District implemented procedures to ensure the health, safety, and welfare of students and compliance with Sections 1006.07, 1006.12, 1006.13, 1011.62(15) and (16), and 1012.584, Florida Statutes.
- Reviewed the audit reports for the five District-sponsored charter schools to determine whether the required audits were performed for the audit period. We also determined whether the 2018-19 fiscal year audits were performed, as applicable, pursuant to Chapters 10.700 and 10.850, Rules of the Auditor General, and Section 1001.453, Florida Statutes.
- Evaluated District procedures and examined District records to determine whether the procedures were effective for distributing the correct amount of local capital improvement funds to eligible charter schools by February 1, 2018, pursuant to Section 1013.62(3), Florida Statutes.
- From the population of purchasing card (P-card) transactions totaling $8 million during the audit period, examined documentation supporting 30 selected P-card transactions totaling $104,699 to determine whether P-cards were administered in accordance with Board policies and District procedures.
- From the population of 89 service contracts with expenditures totaling $19.1 million during the audit period, examined supporting documentation, including the contract documents, for 28 selected expenditures totaling $3 million related to 24 contracts to determine whether:
  - The District complied with competitive selection requirements.

- The contracts clearly specified deliverables, time frames, documentation requirements, and compensation.
- District records documented satisfactory receipt of deliverables before payments were made.
- The payments complied with contract provisions.

- 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

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our operational audit.

Sherrill F. Norman, CPA
Auditor General

School District of Indian River County
6500 57th Street • Vero Beach, Florida, 32967 • Telephone: 772-564-3000 • Fax: 772-564-3054
David K. Moore, Ed.D. - Superintendent

Sherrill F. Noman, CPA
State of Florida Auditor General
Claude Denson Pepper Building, Suite G74
111 West Madison Street
Tallahassee, Florida 32399

August 14, 2020

Reference: 2018-2019 Operational Audit Responses

Dear Ms. Norman,

Pursuant to your letter dated July 30, 2020 regarding the 2018-2019 Operational Audit for the School District of Indian River County, please find below our written explanation and corrective action plans. The operational audit was for the fiscal year ending June 30, 2019.

- Finding 1, 2 and 3 were corrected for 2019-20 FY.
- Finding 4 and 6, corrective actions plans have been initiated in 2020-21 SY.
- Finding 5 has been reviewed and verification protocol have been put in place to safeguard the district.

Finding 1: District school safety policies and procedures need improvement.

Regarding frequency of safety drills:

1. Memorandum dated March 23, 2018 from Governor Rick Scott defined active shooter drill frequency of one per semester.
2. During a meeting held February 26th, 2019 the district elected to conduct active shooter drills monthly for the remainder of the year.
3. Memorandum from Florida Department of Education dated May 31, 2019 defined active shooter drill frequency as one per month.

Corrective action has been implemented to address the finding.

1. The superintendent issued a management directive on August 9th, 2019 for all schools to follow regarding school hardening and harm mitigation safety drills.
2. Changes to Board Policy 8420 were adopted in September of 2019 to include language contained in SB 7026.
3. The district implemented enhanced communication protocols containing weekly briefings to schools outlining emergency drill requirements.

Finding 2: District controls over payments for School Resource Officers (SRO) could be enhanced. Finding was corrected in 2019-20.

During the audit it was discovered the SRO's were not checking in the front office of the school each day. They were however, checking in with their supervisor and the law enforcement agency was ensuring there was an officer at all locations. If an officer was out, a substitute officer was assigned.
During the audit of the payment for these services it was observed that the invoices were paid without additional verification that the services were provided. Internal controls are in place to ensure every school

has an SRO every school day through direct communication between the district, schools and the law enforcement agencies. The district implemented procedures for 2019-2020 with timesheets at each school for SRO's to sign in and out each day. The principal verifies timesheets for accuracy and forwards to Director of Security and Emergency Operations who verifies timesheets and invoice for accuracy and approves for payment. Accounts Payable receives invoice and approved timesheet documentation for payment processing. The sign in sheets are consolidated monthly by school and used to validate the monthly services and payments for services.

Finding 3: The District did not always provide financial reports monthly to the Board. Such reports provide the Board with information needed for policy decisions. Finding was corrected in 2019-20.

The District elected to move from "TERMS" enterprise resource accounting system to "Focus" in January 2019. After the integration from the prior system and going-live in the new "Focus" system, it was discovered that several accounting processes and workflows were not working correctly, and the system was not able to report accurate financial information. From December to June 2019 the focus of the district was to correct the deficiencies and work in collaboration with the Focus team to correct all accounting processes, workflows and financial reporting issues. All major issues and deficiencies have been resolved.

- On November 20, 2018 the district submitted financial statements to the Board for the period of July 1, 2018 to September 30, 2018.
- On April 23, 2019, the district submitted financial statements to the Board for the period of October 1, 2018 to December 31, 2018.
- On June 11, 2019 the district submitted financial statements to the Board for the period ending January 31, 2019.
- On September 10, 2019, the district submitted financial statements to the Board for the period of February, March, April, and May 2019.
- On September 24, 2019, the district submitted the Annual Financial Report for the fiscal year ended June 30, 2019.

Effective July 1, 2019 for the fiscal year 2019-20, enhanced and improved monthly financial statements have been reported to the Board and placed on the district website as required by State Board of Education (SBE) Additional improvements in the district's monthly financial reporting is also under development that will provide the board, community and stakeholders with additional information to make effective and efficient financial decisions.

Finding 4: Some unnecessary Information Technology (IT) user access privileges existed that increased the risk that unauthorized disclosure of sensitive personal information of students may occur.

The District agrees with the finding and corrective measures will be put in place to address in the 2020-21 School Year. A comprehensive review of all access privileges will be conducted and compared the scope of work required for each position/user and the data required by the user to complete their task access will be immediately removed from any user found with unnecessary privileges.

IT system access protocols will be developed to hide sensitive information, create alternative reporting options or reconfigure information for user's needs. The District will implement IT process to ensure that access to sensitive personal information of students is properly safeguarded, and document periodic evaluations of IT user access privileges to determine whether such privileges are necessary and to ensure the timely removal of any inappropriate or unnecessary access privileges are detected. If an individual only requires occasional access to sensitive personal student information, the privileges should be granted only for the time needed and will be automatically removed at a predetermined date.

The District will upgrade the SIS access protocols to include a mechanism to differentiate between IT user access privileges to current student information from access privileges to former student information.

The District will implement protocols to ensure only those employees with a demonstrated need to access the sensitive personal information of students have such access.

Finding 5: Some inappropriate or unnecessary IT access privileges were granted to District employees. A similar finding was noted on our report No. 2017-095.

In order to ensure accurate and timely processing of all payroll cycles we have granted the Districts' payroll manager emergency access to correct salary calculation, supplements, etc. The access is on an emergency-basis only. If an error is discovered during the payroll process, the payroll manager's protocol is to first contact the Human Resource's compensation personnel to review and make the correction. If they are unavailable and the timeline to process the current payroll cycle is critical, the payroll manager will make the corrections and finalize the payroll process. The payroll manager will then follow-up with the Human Resource's compensation personnel to verify and confirm the adjustment was correct. The District understands the exposure and supports the payroll manager having this additional access to address any last-minute errors during the payroll process, with the follow-up and verification protocol. The District views this as an acceptable risk. Any of these emergency corrections are immediately communicated and verified by Human Resources compensation personnel.

Finding 6: The District had not established a comprehensive IT risk assessment.

The District agrees with the finding and corrective measures have been put in place to address. A comprehensive IT Risk plan will be started in the 2020-21 School Year.

Sincerely,

David K. Moore, Ed.D.
Superintendent