STATE OF FLORIDA AUDITOR GENERAL

Operational Audit

Report No. 2017-053
November 2016

SANTA ROSA COUNTY DISTRICT SCHOOL BOARD

Sherrill F. Norman, CPA
Auditor General

Board Members and Superintendent

During the 2015-16 fiscal year, Timothy S. Wyrosdick served as Superintendent of the Santa Rosa County Schools and the following individuals served as School Board Members:

	District No.
Diane L. Scott, Ph.D.	1
E. Hugh Winkles, Chair to 11-17-15	2
Carol Boston	3
Jennifer G. Granse, Chair from 11-18-15, Vice Chair to 11-17-15	4
Scott T. Peden, Vice Chair from 11-18-15	5

The team leader was Barbara J. Sturdivant, CPA, and the audit was supervised by Kenneth C. Danley, CPA. For the information technology portion of this audit, the team leader was Sue Graham, CPA, CISA, and the supervisor was Heidi G. Burns, CPA, CISA.

Please address inquiries regarding this report to Micah E. Rodgers, CPA, Audit Supervisor, by e-mail at micahrodgers@aud.state.fl.us or by telephone at (850) 412-2905.

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

www.myflorida.com/audgen

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

SANTA ROSA COUNTY DISTRICT SCHOOL BOARD

SUMMARY

This operational audit of the Santa Rosa County School District (District) focused on selected District processes and administrative activities and included a follow-up on findings noted in our report No. 2014-131. Our operational audit disclosed the following:

Finding 1: Required background screenings for contractor employees were not always performed at least once every 5 years and documented.

Finding 2: The District needs to improve controls over contractual service agreements and related payments. A similar finding was noted in our report No. 2014-131.

Finding 3: The virtual instruction program provider contract did not contain certain necessary provisions. A similar finding was noted in our report No. 2014-131.

Finding 4: Some inappropriate or unnecessary information technology (IT) access privileges existed that increased the risk that unauthorized disclosure, modification, or destruction of District data and IT resources may occur. In addition, the District had not established procedures for the review of certain IT access privileges to promote the timely detection of inappropriate or unnecessary privileges.

Finding 5: The District did not timely remove the IT access privileges of some former employees.

Finding 6: Certain IT security controls related to user authentication, monitoring of network activity, and data loss prevention need improvement to ensure the continued confidentiality, integrity, and availability of District data and IT resources. Similar findings were noted in our report No. 2014-131.

Finding 7: The District did not have a comprehensive, written IT security incident response plan.

Finding 8: The District did not have a comprehensive, written IT risk assessment plan.

BACKGROUND

The Santa Rosa 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 Santa Rosa County. The governing body of the District is the Santa Rosa County District School Board (Board), which is composed of five elected members. The elected Superintendent of Schools is the executive officer of the Board. During the 2015-16 fiscal year, the District operated 34 elementary, middle, high, and specialized schools; sponsored 2 charter schools; and reported 26,236 unweighted full-time equivalent students.

This operational audit of the District focused on selected processes and administrative activities and included a follow-up on findings noted in our report No. 2014-131. The results of our audit of the District's financial statements and Federal awards for the fiscal year ended June 30, 2016, will be presented in a separate report.

FINDINGS AND RECOMMENDATIONS

Finding 1: Background Screenings

State law[1] provides that instructional and noninstructional contractors who are permitted access on school grounds when students are present or who have direct contact with students must undergo a level 2 background screening[2] at least once every 5 years. State law[3] also provides that noninstructional contractors may be exempt from the background screening requirement if the contractors are under the direct supervision of a school district employee or contractor who has had a criminal history check and meets the statutory background screening requirements.

To promote compliance with the statutory background screening requirements, Board policies[4] require applicable contractors and their workers to undergo required background screenings at least once every 5 years and, according to District personnel, efforts are made to verify initial background screenings. However, District personnel indicated that they did not maintain a comprehensive list of the contractor workers to ensure that background screenings are obtained and evaluated at least once every 5 years.

The Board routinely contracts for instructional substitute teacher services and noninstructional custodial, food, and transportation services. According to District records for the 2015-16 fiscal year, 1,630 contractor workers provided these services and were permitted access on school grounds when students were present or had direct contact with students. However, our analysis disclosed that, as of June 30, 2016, District records did not demonstrate that background screenings for 85 contractor workers[5] had been performed at least once in the past 5 years and, in response to our inquiry, District personnel indicated that the contractor workers were not exempt from the background screening requirements. As of June 30, 2016, periods ranging from 5 years and 16 days to 14 years and 10 months had elapsed since the 85 individuals' most recent background screenings. In response to our inquiries in October 2016, District personnel indicated that some of the 85 workers are no longer employed by the contractors but, for those still employed, the District is obtaining evidence of the required background screenings.

Absent effective controls to ensure that required background screenings are performed, there is an increased risk that contractor workers with unsuitable backgrounds may be allowed access to students.

[1] Sections 1012.465 and 1012.467, Florida Statutes.

[2] A level 2 background screening includes fingerprinting for Statewide criminal history records checks through the Florida Department of Law Enforcement and national criminal history records checks through the Federal Bureau of Investigation, and may include local criminal records checks through local law enforcement agencies.

[3] Section 1012.468, Florida Statutes.

[4] Board policies 3.68 Background Screening for Contractors and 6.17 Appointment or Employment Requirements.

[5] The 85 contractor workers included 35 instructional substitute teacher, 31 noninstructional custodial service, and 19 noninstructional food service contractor workers.

Recommendation: The District should take immediate action to identify all contractor workers who have not obtained the required background screenings, ensure the background screenings are promptly obtained and evaluated, and make decisions as necessary based on evaluations of the background screenings. To help monitor and ensure that required background screenings are performed at least once every 5 years, we recommend that the District maintain a comprehensive, up-to-date list of contractor workers subject to the screenings.

Finding 2: Contractual Services

Effective contract management ensures that contract provisions establish required services and related service times and satisfactory receipt of contracted services before payment. The Board routinely enters into contracts for services, and internal controls have been designed and implemented that generally ensure payments are consistent with contract terms and provisions.

For the 2015-16 fiscal year, contractual services payments totaled $38.1 million and, to determine the propriety of these payments, we examined District records supporting 17 selected payments totaling $4.8 million related to 15 contracts. While District controls over contractual services and related payments were generally adequate, we found that payments related to contracts with the Santa Rosa County Sheriff's Office (Sheriff's Office) and the City of Gulf Breeze (City) for school resource officer (SRO) services could be enhanced.

Pursuant to State law,[6] the Board entered into contracts with the Sheriff's Office and the City for SRO services. The contract with the Sherriff's Office was for SRO services at seven schools, including a K-9 unit at one of the schools, and the contract with the City was for SRO services at two schools. For the 2015-16 fiscal year, the District paid the Sheriff's Office and the City a total of $390,776 for SRO services based on invoices approved for payment by the Middle School Department Secretary. The SRO contracts were fixed-price contracts that required the SROs to be on duty and on-site each day school was in session from 30 minutes before the students' school day started until 30 minutes after the school day ended. Further, for the SRO 2015-16 fiscal year services, the District fully paid the Sheriff's Office and the City in April 2016 and May 2016, respectively. As a result, for the Sheriff's Office and City SRO services, the District prepaid $58,503 for 32 school days and $4,113 for 12 school days, respectively. However, District personnel with direct knowledge of the SRO services did not maintain sign-in, sign-out sheets or other records to demonstrate that the SRO services were satisfactorily received within the required service times.

In response to our inquiries, District personnel indicated that they were confident the SRO services were satisfactorily received within the required service times for the 2015-16 fiscal year, but will consider enhancing documentation requirements for future SRO services. Without evidence that SRO services are satisfactorily received within the required service times and before payments are made, the risk increases that overpayments may occur or that services provided may be inconsistent with Board expectations. A similar finding was noted in our report No. 2014-131.

Recommendation: The District should establish procedures to require and ensure that documentation of the satisfactory receipt of SRO services is received within the required service times before payments are made for the services.

[6] Section 1006.12, Florida Statutes.

Finding 3: Virtual Instruction Program – Contract Provisions

State law[7] requires that each contract with a Florida Department of Education (FDOE) approved virtual instruction program (VIP) provider contain certain provisions. In addition, to ensure appropriate controls over data quality, security measures, and provider contract compliance, VIP provider contracts need to contain other necessary provisions to establish the District's expectations for these providers.

During the 2015-16 fiscal year, the District had 26 full-time and 9 part-time students participating in a FDOE-approved VIP provider program. Our review of the District's contract with the FDOE-approved VIP provider, along with other related records, disclosed that:

- The contract did not include data quality requirements. The provider is to maintain significant amounts of education data used to support the VIP administration and to meet District reporting needs for compliance with State funding, information, and accountability requirements in State law.[8] Accordingly, it is essential that accurate and complete data maintained by the provider on behalf of the District be readily available. Inclusion of data quality requirements in the provider contract would help ensure that District expectations for the timeliness, accuracy, and completeness of education data are clearly communicated to the provider.
- The contract did not specify any minimum required security controls the District considered necessary to protect the confidentiality, availability, and integrity of critical and sensitive education data. While the contract contained requirements for the provider to implement, maintain, and use appropriate administrative, technical, or physical security measures required by Federal law,[9] without specified minimum required security controls, there is an increased risk that provider information security and other information technology (IT) controls may not be sufficient to protect the education data.
- The contract did not provide for the District's monitoring of provider compliance with contract terms or quality of instruction. Without such a provision, District personnel may be limited in their ability to perform monitoring. Such monitoring could include confirmation or verification that the VIP provider protected the confidentiality of student records and supplied students with necessary instructional materials.

In response to our inquiries, District personnel indicated the District no longer employs the former Coordinator of VIP who was responsible for the 2015-16 VIP contract provisions, and are unaware why the contract provisions were excluded. District personnel also indicated that they would consider inclusion of the provisions in future VIP provider contracts. A similar finding was noted in our report No. 2014-131.

Recommendation: The District should ensure that the FDOE-approved VIP provider contract includes data quality requirements, provisions specifying the minimum required security controls, and a provision for monitoring provider compliance with contract terms and quality of instruction.

[7] Section 1002.45(4), Florida Statutes.

[8] Section 1008.31, Florida Statutes.

[9] The Family Educational Rights and Privacy Act (Title 20, Section 1232g, United States Code).

Finding 4: Information Technology – Access Privileges

Access controls are intended to protect District data and IT resources from unauthorized disclosure, modification, or destruction. Effective access controls include granting 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 their areas of responsibilities. Periodically reviewing assigned IT access privileges helps ensure that employees cannot access or modify IT resources inconsistent with their assigned job duties.

Our tests of selected access privileges to the District's business application, including finance and human resources (HR), supporting infrastructure (i.e., mainframe), and network disclosed that some access privileges permitted an employee to perform incompatible functions or were unnecessary and that the District did not have procedures in place for the review of IT access privileges granted to the business application and supporting infrastructure and the administrator privileges granted to network accounts. Specifically:

- Our test of the appropriateness of all business application access privileges granted for the District's two business application security administrators disclosed that the District's Management Information Analyst had update access privileges defined for all 50 security bytes[10] that are used to control access to each screen or menu within the finance and HR transactions. These access privileges were contrary to an appropriate separation of IT technical support responsibilities, including application programming and security administration, and application end-user responsibilities.
- Our test of the four default network administrator system groups[11] that allow complete access to network resources resulted in the review of 10 service and 5 user accounts and one user group. Our review disclosed 1 service account that was no longer necessary for District operations had been granted administrator privileges within the District's network domain.[12] Administrator access privileges are typically limited to employees who are responsible for performing network administration duties or services that require complete access to network resources. In response to our audit inquiry, District management disabled the service account.
- Although the District security administrator responsible for granting and administering access privileges for the business application biannually reviewed the appropriateness of employee access privileges, reviews of employee access privileges granted for the business application were not being performed by supervisory end-user personnel to ensure that access privileges assigned continue to be authorized and appropriate. In addition, District management had not performed a review of administrator access privileges assigned to network accounts.
- According to the District's mainframe security administrator, a review of all mainframe accounts is performed annually and any account that has not been used within that year is suspended. Further, all accounts that have been suspended for at least 1 year are deleted. However, our extended audit procedures for 35 mainframe accounts disclosed that 19 of the accounts had not been used for a period ranging from 3 to 12 years and were not disabled. These 19 accounts had either the Customer Information Control System privilege assigned to log on to the

[10] Security bytes indicate if a user has access to inquire or update screens or menus. Special values are also used to indicate limited inquiry to portions of a screen or menu or limited update to portions of a screen or menu.

[11] Groups are used to combine user accounts, automated system services accounts, and, in some cases, other groups into one unit in order to share assigned permissions.

[12] A domain is a form of a computer network in which all, or a portion of, user accounts, computers, printers, and other IT resources are centrally clustered together to facilitate centralized administration and maintenance of the IT resources.

mainframe, the JOB privilege assigned to run batch jobs, or a combination of both privileges. District management stated that, subsequent to our inquiry, these accounts were either deleted or suspended, as appropriate.

Unnecessary IT access privileges and the lack of a review of IT access privileges granted to the business application and supporting infrastructure and the administrator privileges granted to network accounts increase the risk that unauthorized disclosure, modification, or destruction of District data and IT resources may occur.

Recommendation: The District should ensure that IT access privileges granted are necessary and enforce an appropriate separation of duties. In addition, the District should enhance procedures for the review, independent of the security administrators, of IT access privileges granted to the business application and supporting infrastructure and develop procedures for the review of IT access privileges for network accounts granted administrator privileges. Any unnecessary or inappropriate access privileges detected during such reviews should be timely removed.

Finding 5: Information Technology – Timely Deactivation of Access Privileges

Effective management of IT access privileges includes the timely deactivation of employee IT access privileges when an employee is reassigned or separates from employment. Prompt action is necessary to ensure that the access privileges are not misused by former employees or others to compromise data or IT resources.

District procedures provide that HR Department personnel e-mail personnel agendas from each Board meeting to the District IT security administrators, and the IT security administrators or their designee review the agendas for transfers, terminations, and position or responsibility changes so that appropriate action regarding employee access can be taken. However, these procedures do not require the immediate removal of access after individuals separate from District employment.

Our tests of District records for the 13 employees with access to the network and either District finance or HR applications who separated from District employment during the 2015-16 fiscal year disclosed that:

- The application access privileges for 12 of the former employees remained active from 18 to 330 days after employment separation.
- The network access privileges, providing access to potential sensitive or confidential files, for 9 of the former employees remained active from 2 to 33 days after employment separation.

In response to our inquiries, District personnel indicated that the untimely removal of application access privileges occurred because the IT security administrators fell behind in removing the application access of former employees. Although our tests did not disclose any errors or fraud as a result of the untimely deactivations, without timely removal of access privileges, the risk is increased that access privileges may be misused by former employees or others.

Recommendation: The District should enhance its procedures and prioritize efforts to ensure that the access privileges of former employees are promptly deactivated.

Finding 6: Information Technology – Security Controls – User Authentication, Monitoring of Network Activity, and Data Loss Prevention

Security controls are intended to protect the confidentiality, integrity, and availability of District data and IT resources. Our audit procedures disclosed that certain District security controls related to user authentication, monitoring of network activity, and data loss prevention need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising District data and IT resources. However, we have notified appropriate District management of the specific issues.

Without adequate security controls related to user authentication, monitoring of network activity, and data loss prevention, the risk is increased that the confidentiality, integrity, and availability of District data and IT resources may be compromised. Similar findings were noted in our report Nos. 2011-133 and 2014-131.

Recommendation: The District should improve security controls related to user authentication, monitoring of network activity, and data loss prevention to ensure the continued confidentiality, integrity, and availability of District data and IT resources.

Finding 7: Information Technology – Security Incident Response Plan

IT security incident response plans are established by management to ensure an appropriate, effective, and timely response to security incidents. These written plans typically detail responsibilities and procedures for identifying, logging, and analyzing security violations and include a centralized reporting structure, provisions for a team trained in incident response, notification to affected parties, periodic review of critical system resources to ensure continued integrity, and incident analysis and assessment of additional actions needed.

Although District personnel indicated informal procedures existed for addressing security incidents, including procedures to identify, classify, contain, investigate, report, and respond to IT security incidents, the District had not developed a comprehensive, written IT security incident response plan. Such a plan could include, among other things:

- Procedures for capturing and maintaining events associated with a security incident.
- The process for involving the appropriate local, State, and Federal authorities.
- The process for notifying, pursuant to State law,[13] applicable parties when a breach of security of confidential personal information has occurred or is reasonably believed to have occurred.
- Identification of security incident response team members and training requirements with regard to the team member roles and responsibilities.

Should an incident occur that involves the potential or actual compromise, loss, or destruction of District data or IT resources, the lack of a comprehensive, written IT security incident response plan may result in the District's failure to take appropriate and timely action to prevent further loss or damage to the District's data and IT resources. In response to our inquiry, District personnel indicated that although

[13] Section 501.171, Florida Statutes.

they believed the District's current procedures are adequate, the District will consider developing a comprehensive, written IT security incident response plan.

Recommendation: To provide reasonable assurance that the District will timely and appropriately respond to events that may jeopardize the confidentiality, integrity, or availability of District data and IT resources, the District should develop a comprehensive, written IT security incident response plan. At a minimum, the plan should include:

- **Procedures for capturing and maintaining applicable events.**
- **The process for involving appropriate authorities.**
- **The process for notifying applicable parties of a security breach.**
- **Identification of response team members and training requirements with regard to the team member roles and responsibilities.**

Finding 8: Information Technology – Risk Assessment Plan

Management of IT-related risks is a key part of enterprise IT governance. Incorporating an enterprise perspective into day-to-day governance actions helps entity personnel understand the greatest security risk exposures and determine whether planned controls are appropriate and adequate to secure IT resources from unauthorized disclosure, modification, or destruction. IT risk assessments, including the identification of risks and an evaluation of the likelihood of threats and severity of threat impact, help support management's decisions in establishing cost effective measures to mitigate risk and, where appropriate, to formally accept residual risk.

Although the District had informally considered external and internal risks to its IT resources, the District had not developed a comprehensive, written IT risk assessment plan. A comprehensive, written IT risk assessment plan would consider specific threats and vulnerabilities at the District, system, and application levels. A comprehensive, written IT risk assessment would also document the range of risks that District systems and data may be subject to, including those posed by internal and external users, as well as plans for the mitigation of identified risks. The absence of a comprehensive, written IT risk assessment plan may lessen the District's assurances that all likely threats and vulnerabilities have been identified, the most significant risks have been addressed, and appropriate decisions have been made regarding which risks to accept and which risks to mitigate through appropriate controls. In response to our inquiry, District personnel indicated that although they believed the District's current procedures and a November 2012 external network vulnerability assessment were adequate, the District will consider developing a comprehensive, written IT risk assessment plan.

Recommendation: To provide a documented framework for managing IT-related risks, we recommend that the District develop a comprehensive, written IT risk assessment plan.

PRIOR AUDIT FOLLOW-UP

The District had taken corrective actions for findings included in our report No. 2014-131, except as noted in Findings 2, 3, and 6 as shown in Table 1.

Table 1
Similar Findings Also Noted in Previous Audit Reports

Finding	Operational Audit Report No. 2014-131, Finding	Operational Audit Report No. 2011-133, Finding
2	5	Not Applicable
3	10	Not Applicable
6	16	11

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 March 2016 to October 2016 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 previous audit reports.
- 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 2015-16 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 the District's 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.
- Reviewed District procedures for maintaining and reviewing access to IT resources. We tested selected access privileges to the District's business application, including finance and human resources (HR), 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 administrator accounts for the network and business application to determine whether these accounts had been appropriately assigned and managed. Specifically we:
    - Tested the six menus or screens that allowed update access privileges to selected critical finance functions resulting in the review of the appropriateness of access privileges granted for 131 accounts.
    - Tested the six menus or screens that allowed update access privileges to selected critical HR functions resulting in the review of the appropriateness of access privileges granted for 114 accounts.
    - Tested the four default network administrator system groups that allow complete access to network resources resulting in the review of the appropriateness of administrator access privileges granted to 15 accounts and one user group for the network.

- Tested the appropriateness of all business application access privileges granted for two business application security administrators by examining access privileges defined for all 50 security bytes that are used to control access to each screen or menu within the finance and HR applications.
- Tested the 7 accounts granted security administrator access privileges for the mainframe.

- Reviewed District documentation to determine whether authentication controls were configured and enforced in accordance with IT best practices. Specific to the mainframe, we reviewed the District-defined authentication controls for 838 accounts.
- Reviewed District procedures and reports related to the capture and review of system activity that were designed to ensure the appropriateness of access to and modification of sensitive or critical resources.
- Reviewed the District's disaster recovery plan to determine whether key recovery personnel and their related responsibilities in the event of a disaster had been identified.
- Determined whether District policies and procedures were in effect governing the classification, management, and protection of confidential and sensitive information.
- Reviewed District procedures to prohibit former employees' access to electronic data files. We also reviewed selected access privileges for all 13 former employees with access to finance or human resource applications who separated from District employment during the audit period to determine whether their access privileges had been timely deactivated.
- Determined whether a comprehensive, written IT risk assessment had been developed to document 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 adequacy of District policies and procedures related to security incident response and reporting.
- Evaluated the District data center's physical access controls to determine whether vulnerabilities existed.
- Evaluated Board, committee, and advisory board minutes to determine whether Board approval was obtained for policies and procedures in effect during the audit period and for evidence of compliance with Sunshine law requirements (i.e., proper notice of meetings, meetings readily accessible to the public, and properly maintained meeting minutes).
- Examined District records to determine whether the District had developed an anti-fraud policy and procedures to provide guidance to employees for communicating known or suspected fraud to appropriate individuals. Also, we examined District records to determine whether the District had implemented appropriate and sufficient procedures to comply with its anti-fraud policy.
- Analyzed the District's General Fund total unassigned and assigned fund balances at June 30, 2016, to determine whether the balances were less than 3 percent of the fund's projected revenues, as specified in Section 1011.051, Florida Statutes. We also performed analytical procedures to determine the ability of the District to make its future debt service payments.
- From the population of $12,228,319 total expenditures and $7,657,153 total transfers made 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 $1,084,491 and $7,383,814, respectively, to evaluate District compliance with the restrictions imposed on the use of these resources.
- Examined supporting documentation for selected salary and benefit expenditures totaling $776,142, from the population of $1,804,787 total Workforce Development funds expenditures for

the audit period, 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 100 industry certifications reported for performance funding that were attained by students during the 2014-15 and 2015-16 fiscal years, examined 25 selected certifications to determine whether the District maintained documentation for student attainment of the industry certifications.
- From the population of 193 adult general education instructional students reported for 13,525 contact hours during the Fall 2015 term, examined District records supporting 1,256 reported contact hours for 26 selected students to determine whether the District reported the instructional contact hours in accordance with Florida Department of Education (FDOE) requirements.
- Examined the District Web site to determine whether it included the 2015-16 fiscal year proposed, tentative, and official budgets pursuant to Section 1011.035(2), Florida Statutes.
- Examined supporting documentation to determine whether required internal funds audits for the 2015-16 and 2 preceding fiscal years were timely performed pursuant to SBE Rule 6A-1.087, Florida Administrative Code.
- Examined District records supporting a $20,000 reimbursement made during the audit period from the District to its direct-support organization to determine the legal authority of the transaction.
- From the population of 3,282 employees compensated a total of $70,199,187 from July 1, 2015, through March 10, 2016, examined District records supporting compensation payments totaling $58,313 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.
- From the population of 2,129 instructional personnel and 110 school administrators compensated a total of $92,360,920 during the audit period, examined supporting documentation for 15 selected employees who were paid a total of $782,545 to determine whether the District had developed adequate performance assessment procedures for instructional personnel and school administrators based on student performance and other criteria in accordance with Section 1012.34(3), Florida Statutes, and whether a portion of instructional employee's compensation was based on performance in accordance with Section 1012.22(1)(c)4., Florida Statutes.
- Examined District records for 30 employees selected from the population of 3,282 individuals employed from July 1, 2015, through March 10, 2016, to assess whether personnel were subjected to required background screenings.
- Analyzed District records for the 1,630 instructional substitute teacher and noninstructional custodial, food, and transportation service contractor employees who provided District services for the audit period and were required to have level 2 background screenings, to determine whether the District complied with background screening requirements.
- Examined District policies, procedures, and related records for school volunteers to determine whether the District searched prospective volunteers' names against the Dru Sjodin National Sexual Offender Public Web site maintained by the United States Department of Justice, as required by Section 943.04351, Florida Statutes.
- Evaluated District procedures and examined Department of Highway Safety and Motor Vehicle and District records to assess whether the District ensured that the 289 bus drivers were properly licensed and monitored during the audit period.
- Reviewed District procedures for acquiring health insurance to determine compliance with Section 112.08, Florida Statutes. We also evaluated the procedures for acquiring other types of

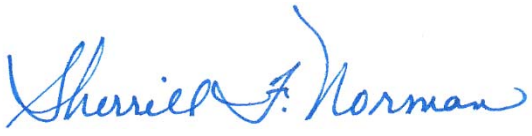
commercial insurance to determine whether the basis for selecting insurance carriers was documented in District records and conformed to good business practice.

- Examined financial records of the District's self-insured health insurance program to determine whether the program was fiscally sound during the audit period.
- Evaluated District procedures for informing the third-party administrator (TPA) of the eligibility of employee and dependent participants. To determine the propriety of District claims expense, we examined District records supporting 30 selected claims totaling $543,669 paid from July 1, 2015, through March 31, 2016, from the paid claims population totaling $7,565,368 that were processed by the TPA, and compared the claims tested to the health insurance program requirements.
- Examined District records supporting the eligibility of 26 selected recipients of Florida's Best and Brightest Teacher Scholarships Program awards from the population of 146 teachers who received scholarships totaling $1.2 million during the audit period.
- From the population of expenditures other than salaries totaling $55,529,726 from July 1, 2015, through March 10, 2016, examined documentation relating to 30 selected expenditures totaling $201,710 to determine whether the expenditures were reasonable, correctly recorded, adequately documented, for valid District purposes, properly authorized and approved, and in compliance with applicable State laws, rules, contract terms and Board policies.
- From the population of purchasing card (P-card) transactions totaling $4,017,867 from July 1, 2015 to May 12, 2016, examined documentation supporting 30 selected transactions totaling $134,041 to determine whether P-cards were administered in accordance with District policies and procedures. We also determined whether the District timely canceled the P-cards for 5 former employees who had been assigned P-cards and separated from District employment during the 2015-16 fiscal year.
- Determined whether rebate revenues for the P-card program totaling $49,661 received for the audit period were allocated to the appropriate District funds.
- Reviewed District policies and procedures related to identifying potential conflicts of interest. For 14 of the 69 employees required to file statements of financial interests, we reviewed Department of State, Division of Corporation, records; statements of financial interests; and District records to identify any potential relationships that represent a conflict of interest with District vendors.
- Examined District records to determine whether the Board had established an adequate, comprehensive electronic funds transfers (EFT) policy and evaluated the adequacy of EFT controls.
- Evaluated the sufficiency of District procedures to determine whether District charter schools and charter technical career centers were required to be subjected to an expedited review pursuant to Section 1002.345, Florida Statutes.
- Reviewed District procedures for evaluating alternative facilities construction methods and significant maintenance-related jobs and identifying cost-effectiveness or efficiency outcomes for applicable personnel in the Administrative Services Department.
- From the population of contractual services payments totaling $38.1 million during the audit period, examined supporting documentation, including the contract documents, for 17 selected contractual services payments totaling $4.8 million related to 15 contracts to determine whether:
  - The District complied with competitive selection requirements;
  - Contracts clearly specified deliverables, time frames, documentation requirements, and compensation;
  - Records documented satisfactory receipt of deliverables before payments were made; and
  - Payments complied with contract provisions.

- Determined whether the District had adequate policies and procedures regarding its Virtual Instruction Program (VIP).
- Evaluated District records for the audit period to determine whether the District provided the VIP options required by Section 1002.45(1)(b), Florida Statutes.
- Examined student records and District procedures for the audit period to determine whether the District ensured that VIP students were provided with all necessary instructional materials and, for those eligible students who did not already have such resources in their home, computing resources necessary for program participation as required by Section 1002.45(3)(c) and (d), Florida Statutes.
- For the FDOE-approved VIP provider that contracted with the District for the audit period, determined whether the District obtained a list of provider employees and contracted personnel who had obtained background screenings in accordance with Section 1012.32, Florida Statutes.
- Examined the contract documents for the FDOE-approved VIP provider to determine whether the contracts contained required statutory provisions. Also, we:
  - Examined the contract documents to determine whether provisions were included to address compliance with contact terms, the confidentiality of student records, and monitoring of the providers' quality of virtual instruction and data quality.
  - Evaluated the contract and other related records to determine whether the District documented the reasonableness of student-teacher ratios established in the contract.
- Evaluated whether the District controls ensured that, pursuant to Section 1002.45, Florida Statutes, the difference in funds provided for a student participating in the District VIP and the price paid for contracted services procured for the audit period was used for implementation of the District digital classrooms plan pursuant to Section 1011.62, Florida Statutes.
- 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

SANTA ROSA COUNTY DISTRICT SCHOOLS

Timothy S. Wyrosdick
Superintendent of Schools
5086 Canal Street Milton, Florida 32570-6706
Phone: 850/983-5012
Cellular: 850/777-7762
Facsimile: 850/983-5013
E-mail:WyrosdickT@.santarosa.kl2.0.us

November 17, 2016

Sherrill F. Norman, CPA
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Ms. Norman:

Pursuant to the provisions of Section 11.45 (4)(d), Florida Statutes, I am submitting to you, in writing, statements of explanation (compiled from the responses as received from those in positions of responsibility of a given area) concerning the items presented in the preliminary and tentative audit findings for the fiscal year ended June 30, 2016. As a matter of organization and clarification, the responses can be referenced using the headings as submitted from your office.

Finding No. 1: Background Screenings

Response: Upon initial inquiry by the AG representative, the District took immediate action to identify all contracted employees and the dates those contracted employees were last submitted for fingerprinting as well as background screenings. The District implemented a policy into the Human Resource Procedures Manual effective August 18, 2016 with School Board approval. As part of this response, the four major contracted vendors were given direct account access to their employees fingerprinting/background screening information and requirements were established for each vendor to keep these lists up to date throughout the year. The District has maintained oversight for all contracted employees in addition to having staff assigned to monitor both contracted employers and their employees for compliance to the newly established policy as well as the fingerprinting/background screening cycles for the same. Contracted employers will now be able to maintain a comprehensive and up-to-date list of their respective employees as well as the District being able to do the same for all employees both contracted and direct.

The School Board has adopted Policy 3.68+ implementing the statutory requirements for screening non-instructional contractors/vendors. All instructional personnel, educational support persons, and non-instructional employees working for a contractor or vendor that is under contract to the School District who have direct contact with students must meet the requirements and comply with all provisions of specified in the Jessica Lunsford Act, F.S. 1012.465, FS. 1012.467, and F.S. 1012.468. Such persons may not be in direct contact with students if ineligible under F.S 1012.315.

The following information is a list of requirements supplied by the District to assist contractors and vendors in bringing their employees into compliance with the required legislation.

• New non-instructional contractors will need to contact the Director of Purchasing and complete the process to become an approved vendor.
• Non-instructional contractors must provide to the Risk Management Safety Specialist a document that includes the name of the company, contact person, phone number, and e-mail address where the designated representative may be reached. The document shall also include the names of all of current employees who will have access to school sites as a part of the contract with Santa Rosa County School District, their social-security numbers, and birth dates. It is required that each non-instructional contractor provide a copy of each employee's completed I-9 document. Employee lists and I-9 documents will be forwarded to the office of Risk Management.
• The District staff member responsible for the management of the contract will contact the non-instructional contractor and identify which employees will be required to be fingerprinted. Those employees with criminal history disclosure must meet the approved background qualification guidelines set by Florida Statute1012.467. Employees who do not meet the guidelines will not qualify to fingerprint and will not be approved to access any School District site or obtain a statewide badge. If it is reported to the School District by FDLE/FBI that an employee has any of the disqualifying charges, they will be denied access to school sites.
• Once contracted employees are identified as being required to fingerprint, the employee will go to the Santa Rosa County District website's "Fingerprinting" page and follow the instructions to complete the fingerprinting process. Individuals will be required to have their original social security card and photo ID to fingerprint.
• It will be the responsibility of the non-instructional contractor to contact the District staff member responsible for the management of the contract to inform the district that an employee has been removed from the company roster. Additionally, if the non-instructional contractor adds a new employee, notification must be made immediately to the District staff member responsible for the management of the contract in writing via email or by fax of the new employee and direct them on the required process prior to the new employee being qualified to fingerprint and reporting to any District site.
• After an employee for a non-instructional contractor has been fingerprinted and their returns have been received by the Risk Management Safety Specialist, the employer will receive verification that the employee was fingerprinted and qualified making them an approved non-instructional contractor employee for five years from their fingerprint date. Each approved employee will receive the uniform statewide badge which MUST be displayed at all times while on the job site, and will be required to show photo identification upon request.
• Non-instructional contractors will be required to update their employee list monthly with the District staff member responsible for the management of the contract to keep information current and up-to-date with the FDLE. All monitoring of non-instructional contractor employees will be the responsibility of the District staff member responsible for the management of the contract. The District will review any arrest information received and the non-instructional contractors will be contacted immediately if the arrest falls within the disqualifiers. If it is determined that an employee is no longer qualified, it will be the contractor's responsibility to permanently remove the employee from the job site or delivery route. The contractor must return the badge to the District within 48 hours of the notification of arrest.

• If a non-instructional contractor has a break in service with the School District, their employees will be monitored for five years from their original fingerprint date, keeping the employees current and up-to-date in the event the company should be awarded a new contract with the District as long as it is within the validity window of the employees' fingerprints. Contractors/vendors/employees will be required every five years to reapply for their statewide badge and will be responsible for any related fees.
• Non-instructional contractors, vendors, and employees are required to sign in at the school office or with the site administrator when accessing District school sites or District offices. District staff will check vendors/contractors and their employees on a regular basis for the uniform state badge to verify identification while on District sites. Employees who cannot produce both of their uniform state badge and a state issued identification upon request will be required to leave the job site immediately, and contractor/vendor employees will be reported to the District staff member responsible for the management of the contract.
• Effective July 1, 2016 any non-instructional contractor employee who does not have the uniform statewide badge will be denied access to school and/or District job sites. In compliance with the Florida Department of Law Enforcement regulations, it is the policy of Santa Rosa County District to not release or supply criminal history record information to the individual who was fingerprinted or the non-instructional contractor who employs the individual. Contractors/vendors are prohibited from requesting, possessing, using and/or maintaining any criminal history record information for any purpose that was generated by Santa Rosa County School District at any time as part of an employee's fingerprinting and background screening process. All future contract provisions with any non-instructional contractors will include this stipulation in writing.

Finding # 2: Contractual Services
Response: The Human Resource department for Santa Rosa County School District and Gulf Breeze Police will send the time sheets for each payroll period to the Director of High Schools electronically. The Director will review, document, and retain these time sheets for each school year. This process has already begun.

Finding # 3: Virtual Instruction Program – Contract Provisions
Response: The following information needs to be included in our contract with future Virtual School providers:

1. Data Quality Requirement for K12 teachers on a monthly basis from K12—timeliness, accuracy.
2. Minimum required security controls.
3. District monitoring of provider compliance with contract terms and quality of instruction.

This process will begin with the renewals of each vendor contract.

Finding # 4: Information Technology – Access Privileges
Response: Update access privileges for the Management Information Analyst to the two business applications will be removed by January 2017. We will begin performing access reviews by end user supervisors to ensure assigned access privileges are authorized and appropriate. Unnecessary or inappropriate access privileges will be removed during account reviews.

Finding # 5: Information Technology – Timely Deactivation of Access Privileges.
Response: Data Processing will recommend to the Administration to add a policy that specifies site administrators contact Data Processing as soon as possible when an employee changes job duties or leaves employment to ensure proper security measures are applied. Data Processing has given security changes top priority to avoid untimely removal of security privileges from user accounts.

Finding # 6: Information Technology – Security Controls – User Authentication, Monitoring of Network Activity, and Data Loss Prevention.
Response: Data Processing agrees with the findings and has made improvements in several areas and is researching options for the remaining findings.

Finding # 7: Information Technology – Security Incident Response Plan.
Response: A Security Incident Response Plan is in development.

Finding # 8: Information Technology – Risk Assessment Plan.
Response: A Risk Assessment Plan is in development.

In conclusion, let me reflect the sincere feeling of our School Board and staff concerning the professional manner in which your staff conducted this audit. In the process of the audit, there always exists a mutual professional respect and consideration of each one's responsibility.

Sincerely,

Timothy S. Wyrosdick
Superintendent of Schools

/lle