THOMAS P. DiNAPOLI
COMPTROLLER

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER
110 STATE STREET
ALBANY, NEW YORK 12236

GABRIEL F. DEYO
DEPUTY COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY
Tel: (518) 474-4037 Fax: (518) 486-6479

August 19, 2014

James Kettrick, Superintendent
Members of the Board of Education
Indian River Central School District
32735-B County Route 29
Philadelphia, NY 13673

Report Number: P3-13-29

Dear Mr. Kettrick and Members of the Board of Education:

A top priority of the Office of the State Comptroller is to help school district officials manage their resources efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support district operations. The Comptroller oversees the fiscal affairs of districts statewide, as well as compliance with relevant statutes and observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving district operations and Board of Education governance. Audits also can identify strategies to reduce district costs and to strengthen controls intended to safeguard district assets.

We conducted an audit of six school districts in central and northern New York State. The objective of our audit was to determine whether the districts adequately control access to their student information system (SIS). We included the Indian River Central School District (District) in this audit. Within the scope of this audit, we examined the District's policies and procedures and reviewed access to the SIS for the period July 1, 2011 through April 30, 2013. We extended our scope period through September 30, 2013 to perform certain tests of the District's access controls.

This report of examination letter contains our findings and recommendations specific to the District. We discussed the findings and recommendations with District officials and considered their comments, which appear in Appendix A, in preparing this report. District officials generally agreed with our findings and recommendations and indicated they planned to initiate corrective action. At the completion of our audit of the six districts, we prepared a global report that summarizes the significant issues we identified at all of the districts audited.

Summary of Findings

The District did not adequately control access to its SIS. Although the Board of Education (Board) established policies related to the confidentiality of computerized information and breach notification requirements, District officials have not established effective procedures for the administration of the SIS to ensure that user access rights are compatible with users' roles or job duties. While there is a formal process to add, deactivate or modify user accounts, management does not periodically monitor user rights to ensure they are current and appropriate. In addition, management does not periodically review change reports or audit logs to identify inappropriate activity in the system. As a result, personal, private and sensitive information (PPSI)[1] in the SIS is at risk of inappropriate access and misuse.

Our audit found that 20 of the 60 user accounts tested (33 percent) included more access rights than necessary for users to fulfill their roles or job duties; these additional rights included adding new student accounts, modifying user rights, changing student demographic information or grades and viewing and modifying health records. Additionally, some users can assume the identity or account of other users, which may give them more access rights than allowed with their own user account. We also compared the District's active employees to a list of current staff users of the SIS and found deficiencies related to 38 user accounts, including six accounts assigned to unidentified users who are not current District employees, 16 generic user accounts that were not assigned to any specific individual and 16 user accounts that were assigned to individuals who are no longer working at the District.

We reviewed audit logs for activities of the 20 users who had more access than necessary and the 38 users who are not current employees or had generic user accounts. Three of the 20 users changed student demographics when it was not their job duty to do so. Additionally, we found 185 changes made under the user account of an inactive employee and one generic user account that accessed the SIS. Lastly, we reviewed 40 grade changes and found one user made 19 grade changes even though it was not their job responsibility to do so.

Our audit also disclosed areas where additional information technology (IT) security controls and measures should be instituted. Because of the sensitive nature of these findings, certain vulnerabilities are not identified in this report, but have been communicated confidentially to District officials so they could take corrective action.

Background and Methodology

The District is located in the Towns of Alexandria, Antwerp, LeRay, Orleans, Philadelphia, Pamelia and Theresa in Jefferson County and the Town of Rossie in St. Lawrence County. It operates eight schools with approximately 4,100 students and 750 employees. The District's budgeted appropriations totaled $80 million for the 2013-14 fiscal year. These costs are funded primarily through State aid, Federal aid and real property taxes.

[1] PPSI is any information to which unauthorized access, disclosure, modification, destruction or disruption of access or use could severely impact critical functions, employees, customers (students), third parties or citizens of New York in general.

The District is governed by a nine-member Board. The Board's primary function is to provide general management and control of the District's financial and educational affairs. The District has a centralized technology department that is headed by the Assistant Superintendent of Curriculum and Instruction (Assistant Superintendent). The Assistant Superintendent is responsible for directing the day-to-day operations of the Technology Department and its staff, which includes overseeing several software applications, including the District's SIS. The Mohawk Regional Information Center (MORIC) houses the District's SIS and provides on-site technical support for the SIS to the District.

The SIS commonly contains extensive information about students, including parent and emergency contacts, attendance, disciplinary actions, testing, schedules, grades and medical information. Therefore, the SIS includes a considerable amount of PPSI, which students and their parents entrust school districts to safeguard. In addition to providing SIS access to teachers, administrators and various staff members, many districts provide parents with limited access to their child's information and students with limited access to their own information.

Authorized users of the District's SIS are parents, students, teachers, administrators and various other District staff,[2] as well as MORIC employees and the SIS vendor who are involved in supporting the SIS. The District assigns access rights through 20 different user groups[3] in its SIS for 1,766 users.[4] Private information in the District's SIS application includes demographic, health, course and special education information; student evaluations; student identification numbers; and current and historical grades. The student data entered into the District's SIS can also be transferred to other operating applications used throughout the District for programs such as school lunch, transportation and special education. Effective controls can help to prevent the misuse and alteration of student information within the SIS and the transfer of incorrect student information to other operating applications within the District.

To achieve our audit objective, we interviewed District officials and staff and examined the District's policies and procedures to control and monitor access to its SIS. We also performed tests to determine if access was properly restricted based on the users' role or job duties and to determine if staff user accounts were assigned to active District employees.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit is included in Appendix B of this report.

Audit Results

District officials are responsible for developing IT controls to protect and prevent improper access to PPSI in the SIS. Policies and procedures should be established to ensure access is limited to only authorized users of the system and that rights assigned to authorized users are

[2] Other staff includes staff for a Pre-Kindergarten program held at the District and staff from the Jefferson-Lewis-Hamilton-Herkimer-Oneida Board of Cooperative Educational Services (BOCES) who provide faculty services to the District.

[3] Comprising 18 instructional and non-instructional staff user groups, one parent group and one student group

[4] Comprising 450 student users, 644 parent users, 629 staff users, 42 MORIC employees and one vendor

compatible with their roles or job duties. Management should periodically monitor user accounts and rights to ensure the rights agree with formal authorizations and are current and updated as necessary. Management should also periodically monitor change reports or audit logs from the SIS for any unusual activity to help ensure that only appropriate changes are being made by authorized users of the SIS.

Policies and Procedures – The Board adopted a Confidentiality of Computerized Information Policy that requires access to confidential computerized data be limited to only authorized personnel of the District. The Board also adopted an Information Security and Breach Notification Policy that clarifies PPSI and details how District employees would notify affected parties whose private information was, or is reasonably believed to have been, acquired without valid authorization.

The District has not adopted written policies and procedures for adding users, establishing users' access rights, deactivating or modifying user accounts and monitoring user access. Although the District has a process in place for adding and changing user rights and utilizes a form to document authorized changes, we found this process was not operating effectively. Individuals were assigned more access rights than they needed for their jobs, and we found numerous user accounts that did not belong to current District employees and should have been deactivated. District officials also do not periodically review users' access rights for appropriateness and do not review audit logs (system-generated trails of user activity) for potentially unauthorized activity. Finally, management does not monitor employees' use of powerful system features that allow them to assume the access rights of other users. Without written procedures over the maintenance of user accounts, staff responsible for these functions may not understand their role, and there is an increased risk that access to the SIS will not be properly restricted.

User Access – When access is not properly restricted, there is an increased risk that sensitive or confidential data will be exposed to unauthorized use or modification. For example, users may be able to view confidential data to which they should not have access or perform functions that they have no authority to do, such as adding a new user account, or modifying student information, such as grades or demographics.

The District has 20 user groups in the SIS, each with an associated set of rights and permissions. The user groups include titles such as Census, Medical, Transportation, Principals and Teachers. The Assistant Superintendent told us all users within a user group have the same rights and permissions to either view or modify data, or both. The District uses a form[5] to document a request and authorization to add a new staff user account, deactivate an account or modify an existing account in the SIS. The form is signed by the user's supervisor and then provided to the Assistant Superintendent who designates the user's role and signs the form to authorize the addition of, or changes to, the user account. The form is then provided to the help desk operator (Operator) in the Technology Department, who determines which SIS user group the user should be placed in and records the group name on the form. A supervisor in the Technology Department then approves the form and it is provided to one of the on-site MORIC employees

[5] Effective January 2012

who are responsible for creating, deactivating and modifying the user account and placing the user in the assigned SIS group(s) as authorized on the form.[6]

We found weaknesses in the District's process for determining what access rights each user should have. When designating the user's role on the form, the Assistant Superintendent chooses one of six different roles.[7] However, this provides limited guidance to the Operator in determining the appropriate user group because there are 20 different user groups which do not necessarily correspond to one of the six roles documented on the form. For example, although there is a "Secretary" role, there is no related "Secretary" group. The Operator told us she assigns a user to a user group based on her historic knowledge of prior users who were assigned the same role. If a staff member needs rights different than those in any established user group, the Operator will assign the staff user to multiple groups to grant additional rights to that user. Although responsible for determining which groups each user should be in, the Operator does not have lists of the individual rights granted to each user group, and there is no process in place to verify that the user's access needs are compatible with the rights of the assigned groups. Further, assigning the same rights to a new user as a predecessor in the same job title/role does not guarantee that the user rights assigned are accurate. Lastly, management does not monitor staff user rights on a periodic basis once rights have been assigned, further increasing the risk that user accounts and rights may not be current or appropriate.

As a result of the weaknesses identified, we compared the access rights/permissions of 60 users in 11 groups[8] to their job duties to determine whether their access was compatible and appropriate. We interviewed 20 of these users who represented each of the groups in our sample to determine their job duties and observed them navigating the SIS modules to see what access was available to them. We found 20 of the 60 users (33 percent) tested had more rights than necessary to fulfill their job duties.[9] Further, the user groups that these users were assigned to indicated that, in fact, the number of users with permissions that are not required for their jobs is much larger. The results of our testing disclosed the following:[10]

- Principals in each of the schools told us that only the high school guidance counselors and principals are authorized to change grades from previous marking periods that have been closed out. A high school guidance counselor told us that high school guidance secretaries assist with recording grade changes in the SIS upon authorization from the guidance counselors. However, in our sample of 60 users, we found four users who can

---

[6] This process does not apply to MORIC user accounts. MORIC has its own process for adding and changing user rights for its employees.

[7] There are four roles listed on the form: Principal, Guidance, Teacher and Secretary. The Assistant Superintendent told us she is aware of two additional roles (Administrator and Medical) that she writes on the form when necessary.

[8] See Appendix B, Audit Methodology and Standards, for details of test selection.

[9] Some staff users had multiple user rights that were not necessary given their job duties. We found that student and parent access rights were appropriate.

[10] MORIC officials told us MORIC SIS support staff require full access rights to the SIS in order to assist the District with troubleshooting on a day-to-day basis. We did not include SIS support staff as exceptions in our testing. However, we did include the SIS vendor and other MORIC technical staff (e.g., programmers and technicians) in our exceptions because they were granted full access rights to the SIS and they only need occasional access for troubleshooting. Rather than provide full access rights to these users all the time, the District should grant them with the necessary access only when they need it.

change closed-out grades (a MORIC employee, system operator, high school psychologist and high school secretary). These four users belong to three different staff user groups. Because user rights and permissions are the same for all users within each user group (as the Assistant Superintendent told us), all the other users within these three user groups are also capable of changing grades. In total, there are 68 users (24 MORIC employees, 43 staff users and the vendor) who can change grades even though it is not within their job responsibilities to do so.

- Nurses and their supervisors are responsible for viewing and modifying health records; however, two other users in our sample (a MORIC employee and the central registrar) could view and modify health records. These two users are in two groups that contain a combined total of 29 users (24 MORIC employees, four staff users and the vendor) who can view and modify health records even though it is not within their job responsibilities to do so.

- The central registrar[11] is responsible for changing student demographic information. However, 19 other users in our sample also have the ability to change demographic information such as student age, student user identification number, address and parent contact information. The 19 users, included in seven user groups, are the system operator, guidance secretary, BOCES occupational therapist, two guidance counselors, clerical aide, building aide, elementary principal, middle school assistant principal, library aide, two high school secretaries, elementary school secretary, high school psychologist, high school principal, high school assistant principal, Assistant Superintendent, transportation secretary and a MORIC employee. Because of the shared user permissions within specific groups, there are 145 users (24 MORIC employees, 120 staff users and the vendor) in these seven user groups who are capable of making changes to student demographic information even though it is not their job duty/responsibility to do so.

- It is the central registrar's responsibility to add a new student account; however, 14 other users in our sample (guidance secretary, BOCES occupational therapist, two guidance counselors, clerical aide, building aide, elementary principal, library aide, two high school secretaries, elementary secretary, Assistant Superintendent, transportation secretary and a MORIC employee) also have permission to add new student accounts. The 14 users are in six user groups that contain a combined total of 109 users (24 MORIC employees, 84 staff users and the vendor) who can add new student accounts even though their responsibilities may not require them to do so.

- It is the MORIC's SIS support employees' responsibility to add new staff user accounts; however, seven other users in our sample (high school principal, high school assistant principal, middle school assistant principal, one elementary school principal, high school psychologist, the system operator and a MORIC technical staff) also have permission to add new staff user accounts. The seven users are in two user groups that contain a combined total of 62 users (24 MORIC employees, 37 staff users and the vendor) who

[11] Onsite MORIC employees serve as a backup for the central registrar.

can add new staff user accounts even though it is not within their job responsibilities to do so.

The Assistant Superintendent told us that the District has not reviewed permissions within the user groups. As a result, our testing found that a significant number of users currently have more access rights in the SIS than they need. The majority of these users are staff, but also include MORIC technical staff (e.g., programmers and technicians) and the SIS vendor who rarely access the SIS to assist the District with troubleshooting and, therefore, do not need all the user rights they have been granted in the SIS. It is important for the District, in conjunction with MORIC, to review and update user permissions in order to help reduce the risk that sensitive or confidential student information could be compromised.

We also compared a list of all the District's active employees to a list of the 629 current staff users of the SIS to determine if any users of the SIS are not District employees or if any former employees remain on the current user list. Of the 629 users, 38 were not on the list of active employees, comprising 16 BOCES and Pre-Kindergarten staff who no longer work at the District, six unknown user account names and 16 user accounts with generic user names not assigned to any one individual. The Assistant Superintendent told us generic accounts should not exist. District officials should deactivate user accounts if they are no longer needed or used, to prevent unauthorized use.

User Activity – Given the weaknesses we identified in the District's process for granting user access rights, we reviewed the District's audit logs[12] for unauthorized user activity during our audit period.

Our review of the audit log activity of the 20 users in our audit sample who had more capabilities in the SIS than their job duties required found that three users (guidance counselor, guidance secretary and high school secretary) made 28 changes to student demographics, even though it is not their job responsibility to do so. Our review of the audit log entries for the other 17 users did not disclose any unauthorized activity.

In addition, we reviewed the audit log activity for the 38 current user accounts that were not assigned to active employees or were generic user accounts. We found 185 changes were made to update attendance records under the user account of an inactive employee after the employee left the District. The Assistant Superintendent subsequently found that the employee's username and password were shared with other employees so they could update the SIS when the employee left the District. The Assistant Superintendent told us staff was directed to use the inactive employee's user account until a replacement was hired in that user's department. Timely deactivation of this account would have prevented other users from accessing it. When accounts are not deactivated as soon as employees leave District service and usernames and passwords are shared, accountability is compromised. We also found that a generic user account was used to view a student's Individualized Education Program (IEP). Because this account was not assigned to a specific individual, District officials do not know who accessed the IEP.

[12] Audit logs are automated trails of user activities, showing when users enter and exit the system and what they did.

We also selected a judgmental sample of 40 final grade changes as shown in the audit log. A MORIC employee who works onsite at the District made 19 changes to students' final grades, even though it is not her responsibility to change grades. The changes to grades included both increases and decreases. For example, changes were made from 89 to 98, 79 to 89, 73 to 96, and 83 to 65. The MORIC employee told us that teachers provided her verbal and/or written lists of grade changes to be made, but she shredded any lists provided after completing the grade changes and, therefore, had no written authorizations or support for the changes. The remaining 21 grade changes were performed by a user who is authorized to make grade changes. Although District officials provided us with verbal explanations for all 40 grade changes selected, they had no formal process for documenting grade changes, including who authorized the changes and the reason for the changes, and for retaining the information on file.

Without documented authorizations to support grade changes and periodic monitoring of audit logs, there is an increased risk unauthorized users could make inappropriate changes to student information without detection.

"Assume-Identity/Assume-Account" Features – The ability to grant or modify user rights in the SIS should be strictly controlled. Individual users should not have the capability to assign themselves additional user rights beyond those already authorized. However, the District's SIS allows certain users to assume the identity or the account of another user.

- The assume-identity feature allows a user to retain their own rights/permissions while accessing student information for students assigned to the user whose identity they assume. During our testing of the sample of 60 users, we identified 13 users[13] in five user groups with the ability to assume identities of another user. In total, these five user groups comprise 89 users (24 MORIC employees, 64 staff users and the vendor) who can perform this assume-identity function.

- The assume-account feature is similar to the assume-identity feature in that the user retains their own rights/permissions. However, it allows a user to assume the account of another user and also inherit all the given rights/permissions of that user. Of the 13 users in our sample who have the ability to assume the identity of another user, 11 users can also assume the account of another user in addition to their own.[14] These 11 users are in three user groups, comprising a total of 83 users (24 MORIC employees, 58 staff users and the vendor) who can perform this powerful function.

Audit logs generated from the SIS appropriately track the activity of users when they assume someone else's identity or account, and the logs show changes made by the actual user. However, the audit logs do not show the user whose identity or account has been assumed and they do not clearly differentiate what actions are completed under a user's assigned account rights versus what actions are taken under an assumed identity or account. This makes it difficult for management to evaluate how often users are using these features and whether they are using

[13] Two guidance counselors, systems operator, guidance secretary, high school secretary, elementary school principal, high school psychologist, middle school assistant principal, high school principal, high school assistant principal, Assistant Superintendent, central registrar and a MORIC employee.

[14] The Assistant Superintendent and the central registrar do not have access to the assume-account feature.

them to make changes or view information that they would otherwise not have access to through their own user account.

Report Monitoring – Audit logs or change reports[15] maintain a record of activity or show changes or deletions made in a computer application. District officials should review these reports to monitor for unusual activity. These reports provide a mechanism for individual accountability and for management to reconstruct events.

Although District officials are aware that audit logs are available in the SIS to review changes made by users, they do not monitor user activity in the SIS with these logs. Because we found that user access was not always assigned according to job duties, it is even more important that the District monitor user activities to ensure appropriate use. When audit logs or change reports are not generated and reviewed, management cannot be assured that unauthorized activities, such as grade changes or adjustments to user account access, are detected and adequately addressed.

Recommendations

1. District officials should review current procedures for assigning user access rights and strengthen controls to ensure that individuals are assigned only those access rights needed to perform their job duties. District officials should monitor user access rights periodically.

2. The Board should adopt written policies and procedures for adding users, establishing users' access rights, deactivating or modifying user accounts and monitoring user access.

3. District officials should evaluate the user permissions currently assigned to each user group, develop a process to verify that individual users' access needs are compatible with the rights of the assigned groups and update the permissions or groups as needed.

4. District officials should deactivate the accounts of any users who are no longer employed at the District.

5. District officials should remove all unused generic or unknown accounts from the SIS.

6. District officials should restrict the ability to make grade changes in the SIS to designated individuals and ensure that documentation is retained to show who authorized the grade change and the reason for the change.

7. District officials should consider whether the assume-identity and assume-account features are appropriate for use. If they decide to use these features, they should work with the SIS vendor to determine if the audit log report format can be modified, or change reports produced, to clearly show user activity performed and all accounts involved when these features are used.

[15] Change reports track specific types of changes made to the system or data.

8. District officials should periodically review available audit logs for unusual or inappropriate activity.

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of the General Municipal Law, Section 2116-a (3)(c) of the Education Law, and Section 170.12 of the Regulations of the Commissioner of Education, a written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and forwarded to our office within 90 days. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. The Board should make the CAP available for public review in the District Clerk's office.

We thank the officials and staff of the District for the courtesies and cooperation extended to our auditors during this audit.

Sincerely,

Gabriel F. Deyo

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

The District officials' response to this audit can be found on the following page.

Indian River Central School District
32735B Co. Rt. 29
Philadelphia, New York 13673

Celebrating Over 50 Years of Academic Excellence

www.ircsd.org

April 23, 2014

Ms. Rebecca Wilcox, Chief Examiner
State Office Building, Room 409
333 East Washington Street
Syracuse, New York 13202-1428

Dear Ms. Wilcox:

I am writing on behalf of the Indian River Central School District in response to the draft audit report (P3-13-29) regarding the Office of the State Comptroller's audit of the District's Student Information System (SIS).

In general, the District is in agreement with the findings of the audit and has already begun to take corrective action to address the recommendations made in the draft report. Unfortunately, some of the findings are beyond our ability to directly address as they are under the purview of the Regional Information Center (MORIC) or the software vendor. Nevertheless, we will take the lead in addressing corrective action that needs to be taken to address the recommendations thoroughly. When necessary, we will actively engage the Regional Information Center and vendor of our SIS in these efforts. These steps will be fully documented, subsequently, in a corrective action plan that the District will submit to the Office of the State Comptroller and the State Education Department.

We appreciate the efforts of the State Comptroller's Office to ensure that the District is exercising safety and security with regard to the access that the District allows its stakeholders to have to its Student Information System.

Sincerely,

James Kettrick
Superintendent of Schools

(315) area code
District Office - 642-3441 High School - 642-3427 Middle School - 642-0125 Intermediate School - 642-0405
Antwerp Primary - 659-8386 Calcium Primary - 629-1100 Evans Mills Primary - 629-4331
Philadelphia Primary - 642-3432 Theresa Primary - 628-4432 District Pupil Personnel Services - 642-0100
Transportation - 642-0331 Building & Grounds - 642-0338 Food Services - 642-1250

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

We reviewed access to the District's SIS for the period July 1, 2011 through April 30, 2013. We extended our scope period through September 30, 2013 to perform certain tests of the District's access controls.

To achieve our audit objective and obtain valid audit evidence, we performed the following audit procedures:

- We interviewed District officials and staff, as well as MORIC staff, to gain an understanding of the District's SIS application and authorized users, assignment and monitoring of user access rights to the SIS, and IT policies and procedures.

- We compared a list of current active employees to a list of current SIS staff users to determine if any users of the SIS are not District employees or if any former employees remain on the current user list. We obtained the most recent employee user list from the SIS and obtained an employee master list from the Payroll Department. We also compared a list of employees who left District employment during our audit period to the list of current SIS users to verify they were no longer active SIS users.

- We selected 60 users of the SIS to compare the users' job duties with user group assignment and individual user rights to determine if access rights are compatible with job duties. We obtained a master list of SIS users and randomly selected 10 percent of instructional and non-instructional staff users (up to a maximum of 50) for a total of 50 users, and judgmentally selected 10 users that we considered to have higher risk. Higher-risk users included those not on the list of current active employees but on the list of SIS users, administrative users, users with add/modify permissions, users who can change closed-out grades, users with access to the medical module and users who have access to assume a user's identity or account.

- We interviewed 20 users to determine what their job duties are and observed them navigating the SIS modules to see what access was available to them.

- We also selected six parent users and five student users to verify that they have just view-only rights as a group and as individuals. We obtained the parent and student user list and randomly selected 1 percent of parent and student users.

- We reviewed the audit logs to determine whether the users identified as exceptions in our tests performed any function that is not part of their job duties or accessed the system after they left the District.

- We selected a total of 40 grade changes, 21 that occurred between the second- and third-quarter marking period and all 19 changes made by a MORIC employee. We determined whether these grade changes were authorized, documented and supported. We focused our testing on the high school for changes made to final grades in marking periods that had already been closed out, excluding grade changes initiated through credit recovery programs.

We conducted this performance audit in accordance with GAGAS. 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 objective.