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

THOMAS P. DiNAPOLI
COMPTROLLER

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

August 19, 2014

Anita Murphy, Superintendent
Members of the Board of Education
Altmar-Parish-Williamstown Central School District
639 County Route 22
P.O. Box 97
Parish, NY 13131

Report Number: P3-13-32

Dear Ms. Murphy 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 located in central and northern New York. The objective of our audit was to determine whether the districts adequately control access to their student information system (SIS). We included the Altmar-Parish-Williamstown 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 November 12, 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 access rights are assigned only to authorized users and are compatible with users' roles or job duties. While there is a formal process to add, deactivate or modify user accounts, and management reviewed non-instructional staff user permissions about two years ago, we found some users had more rights than necessary to perform their job duties. In addition, management does not periodically review change reports and 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 8 of the 35 user accounts tested (23 percent) included more access rights than necessary for users to fulfill their roles or job duties; these additional rights included adding new users, modifying user rights, changing student demographic information or grades and viewing and modifying health records. We also compared the District's active employees to a list of current staff users of the SIS and found 22 generic user accounts that were not assigned to any specific individuals, 12 shared user accounts and 26 user accounts that were assigned to individuals who no longer work at the District. Further, District officials were not sure if change reports were available from the SIS and they were unable to provide a clearly understood audit log report from the SIS. Management did not review any user changes during our audit period.

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 specific 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 Albion, Amboy, Hastings, Mexico, Orwell, Parish, Richland, West Monroe and Williamstown in Oswego County. It operates two schools with approximately 1,300 students and 240 employees. The District's budgeted appropriations totaled $32.1 million for the 2013-14 fiscal year. These costs are funded primarily through State aid and real property taxes.

The District is governed by a seven-member Board. The Board's primary function is to provide general management and control of the District's financial and educational affairs. The Network Administrator is responsible for directing the day-to-day operations of the SIS. The Central New York Regional Information Center (CNYRIC) houses the District's SIS and provides technical support for the SIS.

[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 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 also 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, teachers, administrators and various other District staff, as well as CNYRIC employees who are involved in supporting the SIS. The District assigns access rights through 30 user roles[2] in its SIS for 504 users.[3] 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 or 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 SIS and that rights assigned to authorized users are 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 and 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.

[2] Comprising one instructional staff role, 28 non-instructional staff roles and one parent role
[3] Comprising 83 parent users, 268 staff users and 153 CNYRIC employees

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, we found this process was not operating effectively. Individuals were assigned more rights than needed for their job duties. In addition, District officials do not review user changes for potentially unauthorized activity. 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 30 user roles in the SIS, each with an associated set of rights and permissions. The user roles include titles such as Elementary Office Clerical, Nurse, Transportation and Counselor. The Network Administrator told us once a user is assigned a role, additional rights or changes to rights can be made within the individual user accounts. Therefore, user rights are customizable to each individual user.

The high school guidance counselor and elementary school secretary are responsible for adding new user accounts to the SIS. They told us they learn of personnel changes (e.g., new hires authorized by the Board) through word-of-mouth and add the user accounts to the SIS accordingly. For instructional staff user accounts, the Network Administrator assigns a user role and activates the user account. For non-instructional staff user accounts, the Network Administrator completes a form to assign a user role and individual access rights and permissions. The form is provided to the CNYRIC Help Desk (Help Desk) and the Help Desk employees are responsible for activating and placing the user in the assigned role and for deactivating and modifying user accounts upon notification from the Network Administrator.[4]

When a user requests rights greater than their assigned role or their predecessor, the Network Administrator contacts the user's supervisor to verify user access needs are compatible with the specific rights to be assigned. However, if a user is replacing a former employee, the Network Administrator typically instructs the Help Desk to duplicate the role and access rights of the user's predecessor. 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.

As a result of the weaknesses identified, we compared the access rights/permissions of 35 users to their job duties to determine whether their access is compatible and appropriate. We interviewed 12 of these users who represented various levels of rights and permissions[5] in our sample to determine their job duties and observed them navigating the SIS screens to see what access was available to them. We found 8 of the 35 users (23 percent) tested had more rights

[4] The District does not add CNYRIC user accounts to the SIS; these user accounts are added by the CNYRIC.
[5] See Appendix B, Audit Methodology and Standards, for details of test selection.

than necessary to fulfill their job duties.[6] We then expanded our testing to review various permissions granted to all 421 District staff and CNYRIC users. Specifically, we searched the electronic user access reports for particular permissions, such as the ability to change grades, in order to identify each user who was granted that right in the SIS. We then compared the list of users who were granted the right to the users who were designated by the District to perform the related function to identify those users with unnecessary access rights. The results of our testing disclosed the following:[7]

- The high school and middle school principals told us the guidance counselors and the guidance secretary are authorized to change grades from previous marking periods that have been closed out. In addition, the two elementary school principals are also authorized to change grades. However, we found there are 60 additional users (51 CNYRIC employees and nine staff users) who can change grades even though it is not their responsibility to do so.

- Nurses are responsible for viewing and modifying health records. However, there are 48 CNYRIC users who can also view and modify health records even though it is not their responsibility to do so.

- The high school guidance secretary and the elementary school secretary are responsible for adding new student records and changing student demographic information such as student age, student user identification number, address and parent contact information. We found there are 54 other users (49 CNYRIC employees and five staff users) who can add a new student account and change student demographic information even though it is not their job responsibility to do so.

- The high school guidance secretary, elementary school secretary, Director of Curriculum and Assessments and the special programs secretary are responsible for adding new parent accounts. However, there are 56 other users (50 CNYRIC employees and six staff users) who can add new parent accounts even though it is not their job responsibility to do so. In addition, the high school guidance counselor and an elementary school secretary are responsible for adding new staff user accounts. We found 45 other users (30 CNYRIC employees and 15 staff users) who also have this capability even though it is not part of their job responsibility.

- The Network Administrator and LAN Technician are responsible for resetting staff passwords and activating instructional staff accounts. However, we found 35 users (31 CNYRIC employees and four staff users) who can also perform these functions in the SIS even though it is not within their job responsibilities to do so.

---

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

[7] District officials told us that designated CNYRIC employees require certain access rights in order to assist the District with troubleshooting. We did not include these employees as exceptions in our testing. In addition, if an employee was assigned as a backup person for a designated user, we did not include the backup person in our exceptions.

The Network Administrator told us the District reviewed non-instructional staff user permissions about two years ago and found some users had more rights than necessary to perform their job duties. Any excess rights identified were removed from the users' accounts at that time. However, 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 CNYRIC staff members who have not been designated 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 the CNYRIC, 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 268 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. We found 12 user accounts were shared by 24 people (two people sharing one account each) and 26 user accounts were assigned to individuals who are no longer working at the District. When accounts are not deactivated as soon as employees leave the District and usernames and passwords are shared, accountability is compromised. We also found 22 generic user accounts that were not assigned to any specific individual. The Network Administrator and Director of Curriculum and Assessment told us they did not know why these accounts were established or if they are currently being used. When generic accounts are used, accountability is diminished and activity in the SIS may not be able to be traced back to a single user. District officials should deactivate user accounts if they are no longer needed or used to prevent unauthorized use.

Report Monitoring – Audit logs or change reports maintain a record of activity or show changes or deletions made in a computer application (e.g., grade changes or adjustments to user account access).[8] 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.

District officials do not monitor user activity in the SIS and were not aware of any change reports available to review changes made by users. The District was able to generate a query report based on specific fields we requested, but the report was complex and difficult to use because it did not clearly show what user actions were taken. Because useful audit logs and change reports are not available, District officials would not be able to determine whether there had been any unauthorized activity by the users identified in our audit who had more capabilities in the SIS than their job duties required, or by the 48 current user accounts that were not for active employees. When audit logs or change reports are not generated and reviewed, management cannot be assured that unauthorized activities 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

[8] Audit logs track all user activities, including when users enter and exit the system and what they did. Change reports track specific types of changes made to the system or data.

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, develop a process to verify that individual users' access needs are compatible with their job duties or role and update the permissions as needed.

4. District officials should remove all unused generic or unknown accounts from the SIS. Users should each have their own unique user account and should not share accounts.

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

6. District officials should work with their SIS provider to determine if useful audit log or change reports can be generated to monitor activities. If useful logs or reports can be generated, District officials should periodically review them 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.

ALTMAR PARISH WILLIAMSTOWN
CENTRAL SCHOOL DISTRICT
Mr. Gerry D. Hudson, Superintendent of Schools
639 County Route 22 Parish, New York 13131
(315) 625-5251
ghudson@apw.cnyric.org

"We shall prepare our students for success in an ever changing world"

Rebel Pride Starts Inside

Syracuse Regional Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428

To Whom It May Concern:

This is to notify you that the Altmar Parish Williamstown Central School District in is receipt of the student information system audit Report Number P3-13-32 dated April 1, 2014.

I found the methodology of the audit to be sound and fair; the research and interaction by the auditing team was thorough and conducted pleasantly and respectfully.

I am pleased that no major or threatening findings were discovered and do not dispute the findings made. In fact, these will result in necessary actions that will become best practice for us in the future. At the very least a clearly defined procedure for adding, amending, and deleting authorized users of the SIS (student information system) will be designed and implemented prior to the end of this school year.

Thank you for your help and assistance in strengthening our system of maintaining student data.

Sincerely,

Mr. Gerry D. Hudson,
Superintendent of Schools

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 November 12, 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 CNYRIC 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. Any discrepancies were followed up with appropriate District officials and staff. 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 35 users of the SIS to compare the users' job duties with the users' role 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 for a total of 27 users, and judgmentally selected eight users that we considered to have higher risk. Higher risk users included users who are administrative users, users with add/modify permissions, users who can change historical grades and users who have access to change a student or parent user name or password.

- We interviewed 12 staff users to determine what their job duties are and observed them navigating the SIS screens to see and understand what access was available to them.

- We also selected one parent user to verify the individual user had just view-only rights.

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.