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

Cheryl Steckly, Superintendent
Members of the Board of Education
Lowville Academy and Central School District
7668 State Street
Lowville, NY 13367

Report Number: P3-13-33

Dear Mrs. Steckly 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 Lowville Academy and 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 October 7, 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, management does not periodically monitor user rights to ensure they are current and appropriate. In addition, management does not generate or 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 for inappropriate access and misuse.

Our audit found that 15 of the 34 user accounts tested (44 percent) included more access rights than necessary for users to fulfill their roles or job duties; these additional rights included changing student demographic information or grades, adding users and modifying group access. Additionally, some users can assume the identity or account of other users, which may give them more access rights than allowed within their own user account. We also compared the District's active employees to a list of current staff users of the SIS and found one generic account that was not assigned to any specific individual and two user accounts that were assigned to individuals who are no longer working at the District.

We reviewed audit logs for activities of the 15 users who had more access than necessary, the two users who are not current employees and the one generic user account. We found five of the 15 users changed student demographics or added new staff users when it was not their job duty to do so. Additionally, we found 31 changes made under a user account of an inactive employee. No changes were made using the one generic user account.

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 the 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 Denmark, Greig, Harrisburg, Lowville, Martinsburg, Montague, New Bremen, Pinckney, Turin, Watson and West Turin in Lewis County. It operates one school with approximately 1,390 students and 418 employees. The District's budgeted appropriations totaled $26.3 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 nine-member Board. The Board's primary function is to provide general management and control of the District's financial and educational affairs. The

[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.

Instructional Technology Specialist (IT Specialist) and the Computer Network Manager (Network Manager) are responsible for the day-to-day operations of the SIS. The SIS is housed at the District and the Mohawk Regional Information Center (MORIC) provides 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 that students and their parents entrust school districts to safeguard. In addition to providing 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 MORIC employees and the SIS vendor who are involved in supporting the SIS. The District assigns access rights through 22 different user groups[2] in its SIS for 666 users.[3] Private information in the District's SIS application includes demographic, 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 system 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 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.

[2] Comprising 21 instructional and non-instructional staff user groups and one parent group
[3] Comprising 427 parent users, 197 staff users, 41 MORIC employees and one vendor

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, 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 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 22 user groups in the SIS, each with an associated set of rights and permissions. The user groups include titles such as Administrators, Counseling, Medical, Principals, Census and Teachers. The IT Specialist told us all users within a user group have the same user rights and permissions to either view or modify data, or both. The Superintendent's secretary told us that she uses the Board minutes to identify personnel changes (e.g., new hires authorized by the Board) and she adds user accounts in the SIS accordingly.[4] When a user is added, the SIS automatically sends an email to the IT Specialist and the Network Manager who are responsible for placing the user in a group and for deactivating and modifying user accounts upon notification from the Superintendent's secretary. The IT Specialist told us he places a new staff user in the same group as their predecessor. If a staff user needs rights different than those in any established user group, the IT Specialist will create a new staff user group to grant rights specific to that user.

We found weaknesses in the District's process to ensure users do not have more access rights than needed. There is no process in place to verify all users' access needs are compatible with the specific rights of the group(s) they are placed in because the IT Specialist assigns users to a user group based on his historic knowledge of prior users who were assigned the same role. Assigning the same rights to a new user as a predecessor in the same job title/role does not guarantee 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.

[4] The District does not add MORIC user accounts to the SIS; these user accounts are added by MORIC.

As a result of the weaknesses identified, we compared the access rights/permissions of 34 users in 13 groups[5] to their job duties to determine whether their access is compatible and appropriate. We interviewed 27 of these users who represented each of the groups 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 15 of the 34 users (44 percent) tested had more rights than necessary to fulfill their job duties.[6] 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:[7]

- The high school guidance counselor and Superintendent's secretary told us there are eight users[8] who are authorized to change grades from previous marking periods that have been closed out. However, in our sample of 34 users, we found 12 other users who can also change closed-out grades (the IT Specialist, secondary assistant principal, middle school principal, two high school principal secretaries, the Superintendent's secretary, a high school teacher and five MORIC employees). These 12 users belong to five different staff user groups. Because the IT Specialist told us user rights and permissions are the same for all users within each group, all the other users within these five staff user groups are also capable of changing grades. In total, there are 39 users (25 MORIC employees, 13 staff users and the vendor) who can change grades even though it is not within their job responsibilities to do so.

- The high school guidance office staff and the elementary and middle school secretaries are responsible for changing student demographic information.[9] However 13 other users in our sample also have the ability to change demographic information such as student age, address and parent contact information. The 13 users, included in six staff user groups, are the IT Specialist, secondary assistant principal, middle school principal, high school principal, two high school principal secretaries, one high school teacher, five MORIC employees and the former Superintendent.[10] Because of the shared user permissions within specific groups, there are 46 users (25 MORIC employees, 20 staff users and the vendor) in these six user groups who are capable of making changes to student demographic information even though it is not their job responsibility to do so.

[5] See Appendix B, Audit Methodology and Standards, for details of test selection.
[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] 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 the necessary access only when they need it.
[8] Three guidance counselors, two building secretaries, a guidance counselor secretary, a guidance aid and a MORIC employee
[9] The Superintendent's secretary updates student profiles in the absence of the building secretaries.
[10] The former Superintendent's user account was not deactivated when he left the District.

- The Superintendent's secretary[11] is responsible for adding new staff user accounts. However, we found nine other users in our sample (secondary assistant principal, middle school principal, two high school principal secretaries and five MORIC employees) also have permission to add new staff user accounts. These nine users are in four groups that contain a combined total of 39 users (25 MORIC employees, 13 staff users and the vendor) who can add new staff user accounts even though it is not within their job responsibilities to do so.

- It is the responsibility of the IT Specialist and the Network Manager to modify user group access rights. However, seven other users in our sample (secondary assistant principal, middle school principal and five MORIC employees) also have the ability to modify user group access rights. These seven users are in one staff user group that contain a combined total of 28 users (25 MORIC employees, two staff users and the vendor) who can perform this function even though it is not within their job responsibilities to do so.

The IT Specialist told us that the District has not revisited permissions within the user groups for several years. 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 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 197 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 two user accounts that were assigned to individuals who are no longer working at the District and one generic account that was not assigned to any specific individual. When generic accounts are used, accountability is diminished and activity in the system 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.

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 15 users in our audit sample who had more capabilities in the SIS than their job duties required found that three users (high school guidance secretary, middle school building secretary and an elementary school building secretary) added new staff user accounts, even though it is not their responsibility to add accounts. In addition, two users (the IT Specialist and secondary assistant principal) made 149 combined changes to student

[11] The IT Specialist and the Network Manager add new staff user accounts in the absence of the Superintendent's secretary.

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

demographic information even though it is not their responsibility to do so. Our review of the audit log entries for the other 10 users did not disclose any unauthorized activity.

In addition, we reviewed the audit log activity for the two current user accounts that were not assigned to active employees and the one generic user account. We found 31 changes were made to update attendance records under the user account of one of the inactive employees after the employee left the District. The IT Specialist told us the former employee's log-in information was shared with another employee so the SIS could be updated when the employee left the District. Timely deactivation of this account would have prevented another user 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 found no changes were made using the generic user account.

We also selected a judgmental sample of 10 grade changes as shown in the audit log. The 10 grade changes were performed by users authorized to make grade changes. District officials retained support for the grade changes and provided it to us for our review. Although there is a formal process for documenting and retaining grade changes, there was no documentation of authorization for the changes and the reasons for the changes. Without documented authorizations to support grade changes, there is an increased risk for 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 rights that have already been 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 user rights/permissions while accessing student information for students assigned to the user whose identity they have assumed. During our testing of the sample of 34 users, we identified nine users (secondary assistant principal, middle school principal, Superintendent's secretary, a high school principal secretary and five MORIC employees) in three user groups with the ability to assume identities of another user. In total, these three user groups comprise 34 users (25 MORIC employees, eight 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 nine users in our sample who have the ability to assume the identity of another user, seven[13] can also assume the account of another user. These seven users are in one user group comprising a total of 28 users (25 MORIC employees, two staff users and the vendor) who can perform this powerful function.

[13] The second assistant principal, middle school principal and five MORIC employees

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 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[14] maintain a record of activity or show changes or deletions made in the 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. 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 remove all generic or unknown accounts from the SIS.

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

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.

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

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.

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.

LOWVILLE ACADEMY and CENTRAL SCHOOL
7668 NORTH STATE STREET
LOWVILLE, NEW YORK 13367-1328
Fax: 315-376-1933 Net: www.lowvilleacademy.org

CHERYL R. STECKLY
Superintendent of Schools
Telephone: 315-376-9000

DANIEL J. CUSHING
High School Principal
Telephone: 315-376-9015

PHILOMENA B. GOSS
Elementary School Principal
Telephone: 315-376-9005

SCOTT D. EXFORD
Middle School Principal
Telephone: 315-376-9010

April 22, 2014

Ms. Rebecca Wilcox, Chief Examiner
Syracuse Regional Office
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, NY 13202-1428

Dear Ms. Wilcox:

The purpose of this letter is to provide a response to the draft audit presented to our school district on April 8, 2014. We would first like to express our appreciation for the professional and courteous manner in which your staff conducted its audit responsibilities and we wish to thank the Examiners for their diligence. The district takes all of the findings and recommendations seriously and will continue to strive to ensure that all of our procedures are in line with best practice protocol.

The draft audit centered on information technology security controls. Eight recommendations were made by the auditing team, of those recommendations four have been addressed and corrected. A corrective action plan to address the remaining issues will be developed and forwarded to your attention in the near future.

The Lowville Academy and Central School District remains committed to transparency in its operations and to the implementation of the Comptroller's recommendations. If you need further information, please feel free to contact me.

Sincerely,

Cheryl R. Steckly
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 October 7, 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 34 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 for a total of 24 users and judgmentally selected 10 users that we considered to have higher risk. Higher risk users included users in the groups which are not covered in the random sample, users who are in multiple groups, administrative users, users with add/modify permissions, users who can change grades and users who can modify student profiles.

- We interviewed 27 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 (and the parent group) had just view-only rights.

- We reviewed the audit log 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 10 grade changes that occurred during our audit period and 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, for pass/fail changes and for different courses.

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.