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

Perry Dewey, Superintendent
Members of the Board of Education
Madison Central School District
7303 Route 20
Madison, NY 13402

Report Number: P3-13-31

Dear Mr. Dewey 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. The objective of our audit was to determine whether the districts adequately control access to their student information system (SIS). We included the Madison 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 1, 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 and deactivate user accounts, management does not verify assigned user rights and 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 for inappropriate access and misuse.

Our audit found that 13 of the 21 user accounts tested (62 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 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 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 three generic user accounts that were not assigned to any specific individuals. 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.

We reviewed audit logs for activities of the 13 users who had more access than necessary and the three generic user accounts. We found three users changed student demographics or made grade changes when it was not their job duty to do so. No changes were made using the three generic user accounts.

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 Eaton, Madison and Stockbridge in Madison County and Augusta, Marshall and Vernon in Oneida County. It operates one school with approximately 470 students and 165 employees. The District's budgeted appropriations totaled $9 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 Technology Coordinator is responsible for the day-to-day operations of the SIS. The Mohawk Regional Information Center (MORIC) houses the District's SIS and provides technical support for the SIS to the District.

[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 MORIC employees and the SIS vendor who are involved in supporting the SIS. The District assigns access rights through 18 different user groups[2] in its SIS for 311 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 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.

<u>Policies and Procedures</u> – The Board adopted a Public Access to Records Policy for confidentiality and to prohibit disclosure of certain personal student records. 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 by a person without valid authorization.

[2] Comprising 17 instructional and non-instructional staff user groups and one parent group

[3] Comprising 182 parent users, 87 staff users, 41 MORIC employees and one vendor

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 they 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 (e.g., grades and demographics).

The District has 18 user groups in the SIS, each with an associated set of rights and permissions. The user groups include titles such as Administrators, Transportation, Teachers and Attendance. The Technology Coordinator told us all users within a user group have the same rights and permissions to either view or modify data. The District utilizes a form to document the request to add a new staff user account and the group(s) the user is assigned to. The form is initially completed by the person requesting access to the SIS and then provided to the Technology Coordinator who designates the user's role (group) on the form and signs it. He then adds the user account to the SIS and places the user in the assigned group(s).[4] The Technology Coordinator told us there is no procedure in place to modify user accounts. He deactivates user accounts upon notification of the Board's approval of any resignations. If a staff member needs rights different than those in any established user group, the Technology Coordinator will modify and assign the staff user to multiple groups to grant additional rights to that user or 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 formal management approval of the access rights assigned by the Technology Coordinator. Also, 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 Technology Coordinator 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 that the user rights assigned are accurate. The Technology Coordinator's ability to assign, create, modify, deactivate and authorize user access rights without any management or supervisory review increases the risk that users could be assigned more access rights than needed. 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 21 SIS users in 13 groups[5] to their job duties to determine whether their access is compatible and appropriate. We interviewed 20 of these users[6] who represented each of the groups in our sample to determine what their job duties are and observed them navigating the SIS screens to see what access was available to them. We found 13 of the 21 users (62 percent) tested had more rights than necessary to fulfill their job duties.[7] 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:[8]

- According to the Teacher's Handbook, only the Principal is authorized to change grades from previous marking periods that have been closed out. However, in our sample of 21 users, we found 11 other users who can also change closed-out grades – guidance counselor, Treasurer, kitchen director, office assistant, Committee of Special Education (CSE) chairperson, clerk, social worker, psychologist, typist, the Technology Coordinator and a MORIC employee. These 11 users belong to eight different staff user groups. Because the Technology Coordinator told us user rights and permissions are the same for all users within each user group, all the other users within these eight staff user groups are also capable of changing grades. In total, there are 38 users (24 MORIC employees, 13 staff users and the vendor) who can change grades even though it is not within their job responsibilities to do so.

- It is the responsibility of the elementary and high school secretaries (and the guidance office staff during the summer) to change student demographic information. However, seven 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 seven users, included in five staff user groups, are the Treasurer, kitchen director, clerk, social worker, psychologist, the Technology Coordinator and a MORIC employee. Because of the shared user permissions within specific groups, there are 33 users (24 MORIC employees, 8 staff users and the vendor) in these five user groups who are capable of making changes to student demographic information even though it is not their job responsibility to do so.

- The Technology Coordinator is responsible for adding and deactivating staff user accounts in the staff user groups; however, two other users in our sample (CSE Chairperson and a MORIC employee) also have permission to add and deactivate staff user accounts. The two users are in two user groups that contain a combined total of 28

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

[6] We did not interview the MORIC employee. However, MORIC officials informed us about the SIS responsibilities of their employees.

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

[8] 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.

users (24 MORIC employees, three staff users and the vendor) who can add and deactivate staff user accounts even though it is not within their job responsibilities to do so.

The Technology Coordinator told us that he was not aware that these users had more permissions than necessary. 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 the 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 87 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 87 users, three were not on the list of active employees and had generic user names that were not assigned to any one individual. The Technology Coordinator told us the accounts were created as sample or test accounts. 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 these generic user accounts 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[9] for unauthorized user activity during our audit period.

Our review of the audit log activity of the 13 users in our audit sample who had more capabilities in the SIS than their job duties required found two users (the guidance counselor and an office assistant/teacher aide) made 141 combined changes to student grades even though it is not their responsibility to change grades. We also found that the Treasurer made 10 changes to student demographics, even though it is not her 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 three generic user accounts and found no changes were made using these accounts.

We selected a judgmental sample of 10 of the 141 grade changes to determine whether these grade changes were authorized, documented and supported. The grade changes included changes from 47 to 70, 58 to 70 and 62 to 70. Although District officials provided us with general, verbal explanations for the 10 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

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

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 rights/permissions while accessing student information for students assigned to the user whose identity they assume. During our testing of the sample of 21 users, we identified nine users[10] in seven user groups with the ability to assume identities of another user. In total, these seven user groups comprise 37 users (24 MORIC employees, 12 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 users can also assume the account of another user.[11] These seven users are in four user groups, comprising a total of 35 users (24 MORIC employees, 10 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 them to make changes or view information to which they would otherwise not have access through their own user account.

Report Monitoring – Audit logs or change reports[12] 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.

District officials do not monitor user activity in the SIS and were not aware of any audit logs or change reports available in the SIS to review changes made by users. 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.

[10] Guidance counselor, Treasurer, CSE chairperson, technology coordinator, social worker, two office assistants, a typist and a MORIC employee

[11] A guidance counselor and the Treasurer do not have access to the assume-account feature.

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

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 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.

6. 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.

7. 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.

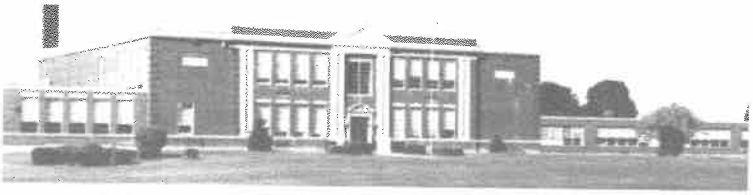
Sincerely,

Gabriel F. Deyo

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

The District officials’ response to this audit can be found on the following pages.



MADISON CENTRAL SCHOOL DISTRICT
7303 Route 20, Madison, New York 13402
Phone: (315) 893-1878
Fax: (315) 893-7111

May 1, 2014

Dear Office of the Comptroller:

Please accept this letter as the written audit response of the Madison Central School District to your draft report of examination letter dated April 30, 2014 ("Draft Report"). After receiving and reviewing your final report, we will prepare a Corrective Action Plan and submit it as required. As noted below, some of the recommendations made in the Draft Report have already been implemented.

We understand that the Office of the State Comptroller conducted an audit of several school districts in Central New York with the specific objective of examining how those districts controlled access to their student information systems (SIS). The inclusion of the District in that study has provided us with an opportunity to examine our procedures and identify areas for improvement. We appreciate the professionalism demonstrated by all staff members of your Office during the examination, and the courtesies extended during the exit meeting.

As your Office is no doubt aware, during the period covered by your examination the primary law governing access to student information was the Federal Family Educational Records and Privacy Act (FERPA). Although not mentioned in the Draft Report, Board Policy 7060 (Student Privacy) and Regulation 7060.1 (Student Privacy – FERPA) have long guided the District's compliance with FERPA. The recommendations in your Draft Report will assist us in continuing this record of compliance into the digital age.

We are pleased that your examination apparently did not identify any circumstance constituting a violation of any state or federal statute or regulation, and that the Draft Report does not identify any instance of inaccurate or fraudulent data alteration. We respect the Comptroller's opinion that the District did not adequately control access to its SIS; albeit, it was unknown to the district that the SIS system operations allowed for these capabilities to be granted to users. We are in general agreement with the recommendations made by your Office, and as noted, have already taken steps to implement some of them.

The District especially appreciates how the Comptroller's audit team worked with our technology partners at the Mohawk Regional Information Center ("MORIC"). Our final assessment of the relative risks and benefits of certain program features discussed in the Draft Report, as well as the technical feasibility of certain recommendations, will be made after further discussion with MORIC staff. We will also work closely with MORIC to develop additional policies or procedures in response to the recommendations in the Draft Report, to insure continued interoperability.

The District agrees with the objective of the Draft Report – that the security and confidentiality of student information be maintained in accordance with all legal requirements. We are confident that the District's Corrective Action Plan will provide a path toward continued improvement.

As of this time, the District has taken corrective action in the areas of access rights and has implemented controls that address several of the recommendations in the Draft Report. In that we are working with the MORIC and SIS provider to correct system security issues as they pertain to the audit logs. The District is also addressing policy and procedures that will address concerns of user rights and access to the SIS system. These items will be expanded upon in our forthcoming corrective action plan.

Sincerely,

Perry T. Dewey
Superintendent

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 1, 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 21 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 10 users, and judgmentally selected 11 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 and users who can change grades.

- We interviewed 20 of these 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 one parent user to verify the individual user (and the parent group) had just view-only rights. We obtained the parent user list and selected an on-site staff person who was a parent.

- 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 10 grade changes made by a guidance counselor who was not designated to change grades in the SIS and determined whether these grade changes were authorized, documented and supported. We focused our testing on changes made to final grades for marking periods that had already been closed out, pass/fail changes and changes made 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.