OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY

Oneida City School District

Controlling Access to the Student Information System

Report of Examination

Period Covered:

July 1, 2014 – October 30, 2015

2016M-53

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

June 2016

Dear School District Officials:

A top priority of the Office of the State Comptroller is to help school district officials manage their districts 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 districts' 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.

Following is a report of our audit of the Oneida City School District, entitled Controlling Access to the Student Information System. This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law.

This audit's results and recommendations are resources for district officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

Office of the State Comptroller
Division of Local Government
and School Accountability

State of New York
Office of the State Comptroller

EXECUTIVE SUMMARY

The Oneida City School District (District) is located in the City of Oneida and the Towns of Lenox and Lincoln in Madison County and the Towns of Vernon, Verona and Vienna in Oneida County. The District is governed by a seven-member Board of Education (Board) that is responsible for the general management and control of the District's financial and educational affairs. The District has a central technology department headed by the Administrator for Technology and Special Programs (Administrator), who is responsible for directing the day-to-day operations and staff. These responsibilities include overseeing the District's Student Information System (SIS). The SIS resides at the District and the Mohawk Regional Information Center (MORIC) provides the District with technical support.

The SIS is an electronic system that serves as the official District record of student performance and is used to track students' grades (entered by District personnel), generate student report cards and maintain student permanent records (i.e., transcripts). It also contains other personal, private and sensitive information (PPSI)[1] about students, including student identification numbers, as well as medical, order of protection and custody information. Authorized users of the SIS are parents, teachers, administrators, various other District employees, District contract counselors, Board of Cooperative Educational Services employees, MORIC employees and the software vendor. The District assigns access permissions to these 322 users through 23 different user groups.[2]

Scope and Objective

The objective of our audit was to examine the District's information technology (IT) access controls over PPSI in its SIS for the period July 1, 2014 through October 30, 2015. Our audit addressed the following related question:

- Did District officials implement IT access controls to adequately safeguard PPSI in its SIS?

Audit Results

Parents and students rely on District officials to ensure that students' PPSI is properly safeguarded. The Administrator, with support from other District and MORIC employees, is responsible for protecting and preventing improper access to this information. To fulfill these responsibilities, the Administrator should monitor audit logs for indications of inappropriate activities which could include inappropriately

[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.

[2] User groups are established in the SIS and permissions are assigned by group. Therefore, all individuals in a group have the same user permissions.

changing student grades, modifying SIS permissions, assuming accounts or identities, or viewing PPSI. The Administrator should ensure users are not granted more permissions than necessary to perform their job duties and user accounts for District and third-party personnel are removed when access to the SIS is no longer needed. To guide these efforts, the Board should develop comprehensive written policies and procedures for reviewing SIS audit logs and managing SIS accounts and permissions.

We identified the following questionable activity and unnecessary permissions granted in the SIS:

- SIS accounts were logged into 81 times from systems that reside outside the United States, which could potentially indicate that those accounts have been compromised. After sharing our findings with District officials, they determined that some of the access was authorized and other access was not. Subsequent to our audit, District officials indicated that they further confirmed 80 of the 81 login events as authorized.

- Guidance counselors and guidance office secretaries changed 48 final course grades from a failing grade to a passing grade without supporting documentation. While none of the grade changes were made by users that do not have the responsibility to change grades, we did find 55 users without such responsibilities that have also been granted permission to change grades in the SIS.

- A keyboard specialist, whose responsibilities include looking up group permissions but not changing those permissions, made seven changes to SIS permissions. Seven other users without the responsibility to manage SIS permissions also have the ability to modify group permissions in the SIS.

- The SIS has functionality that allows users to assume the account or identity of another user. We found that SIS identities were assumed over 2,000 times and SIS accounts were assumed over 200 times by 37 different users. An additional 54 users have also been granted permissions to assume accounts or identities.

- We could not determine whether PPSI has been accessed inappropriately because viewing PPSI is generally not logged in the SIS. However, we did find that 22 users are unnecessarily able to view the Social Security number field in the SIS, 21 users are unnecessarily able to view students' identification numbers, seven users are unnecessarily able to view students' medical information, 50 users are unnecessarily able to view students' order of protection information, 58 users are unnecessarily able to view students' custody information and nine users are unnecessarily able to view PPSI in the SIS audit log.

We also found unnecessary user accounts in the SIS, including six for former District employees, five for former third-party personnel, two for MORIC personnel that do not directly support the SIS and 22 for substitute secretaries and nurses that only need occasional access. These unnecessary accounts increase the risk that an account could be used to inappropriately access the SIS. It also increases the efforts needed to manage permissions in the SIS, which could allow inadvertently granting more access than needed.

Finally, we found that District officials do not review SIS audit logs on a regular basis nor do they properly manage SIS accounts and permissions. In addition, they have not established effective policies and procedures for protecting the PPSI in the SIS. The questionable activity, unnecessary permissions and unnecessary user accounts we identified result, at least in part, from the lack of effective management and monitoring of access to the SIS.

Comments of District Officials

The results of our audit and recommendations have been discussed with District officials and their comments, which appear in Appendix A, have been considered in preparing this report. Except as specified in Appendix A, District officials generally agreed with our recommendations and indicated they planned to take corrective action. Appendix B includes our comments on the issues raised in the District's response letter.

Introduction

Background

The Oneida City School District (District) is located in the City of Oneida and the Towns of Lenox and Lincoln in Madison County and the Towns of Vernon, Verona and Vienna in Oneida County. The District operates six schools with approximately 2,600 students and 550 employees. The District's budgeted appropriations totaled $41 million for the 2015-16 fiscal year. These costs are funded primarily through State aid and real property taxes.

The District is governed by a seven-member Board of Education (Board). The Board is responsible for the general management and control of the District's financial and educational affairs. The District has a central technology department headed by the Administrator for Technology and Special Programs (Administrator), who is responsible for directing the day-to-day operations and staff. These responsibilities include overseeing computer hardware and software applications, including the District's Student Information System (SIS). The SIS resides at the District and the Mohawk Regional Information Center (MORIC) provides the District with technical support.

The SIS is an electronic system that serves as the official District record of student performance and is used to track students' grades (entered by District personnel), generate student report cards and maintain student permanent records (i.e., transcripts). The SIS also contains other personal, private and sensitive information (PPSI)[3] about students, including student identification numbers, as well as medical, order of protection and custody information.

Authorized users of the SIS are parents, teachers, administrators, various other District employees, contract counselors, Board of Cooperative Educational Services (BOCES) employees, MORIC employees and the software vendor. The District assigns access permissions to these 322 users through 23 different user groups.[4]

Objective

The objective of our audit was to examine information technology (IT) access controls over PPSI in the District's SIS. Our audit addressed the following related question:

- Did District officials implement IT access controls to adequately safeguard PPSI in its SIS?

[3] 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.

[4] User groups are established in the SIS and permissions are assigned by group. Therefore, all individuals in a group have the same user permissions.

Scope and Methodology

We examined the District's IT access controls for the period July 1, 2014 through October 30, 2015. Due to the potential sensitivity of some of this information, we did not discuss the results in this report but instead communicated them confidentially to District officials.

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 are included in Appendix C of this report. Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

Comments of District Officials and Corrective Action

The results of our audit and recommendations have been discussed with District officials, and their comments, which appear in Appendix A, have been considered in preparing this report. Except as specified in Appendix A, District officials generally agreed with our recommendations and indicated they planned to take corrective action. Appendix B includes our comments on the issues raised in the District's response letter.

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of General Municipal Law, Section 2116-a (3)(c) of New York State 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 provided to our office within 90 days, with a copy forwarded to the Commissioner of Education. 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.

Access to the Student Information System

Parents and students rely on District officials to ensure that students' PPSI is properly safeguarded. The Administrator, with support from other District and MORIC employees, is responsible for protecting and preventing improper access to this information. To fulfill these responsibilities, the Administrator should monitor audit logs for indications of inappropriate activity. The Administrator should ensure users are not granted more permissions than necessary to perform their job duties and user accounts for District and third-party personnel are removed when access to the SIS is no longer needed. To guide these efforts, the Board should develop comprehensive written policies and procedures for reviewing SIS audit logs and managing SIS accounts and permissions.

We found questionable activity and unnecessary permissions granted for changing student grades, modifying SIS permissions, assuming accounts or identities and viewing PPSI. We also found unnecessary user accounts in the SIS, including those for former District employees, former third-party personnel, MORIC personnel that do not directly support the SIS and substitute secretaries and nurses that only need occasional access. These issues were the result of, at least in part, District officials' failure to review SIS audit logs on a regular basis, properly manage accounts and permissions and establish effective policies and procedures. Unnecessary permissions increase the risk of inappropriate activity, such as unauthorized changes to students' grades or SIS permissions and disclosure or misuse of students' PPSI. Unnecessary accounts also increase this risk, as well as the efforts needed to manage permissions in the SIS, which could result in inadvertently granting more access than needed.

Activity and Permissions

The Administrator is responsible for preventing and monitoring for improper access to and use of the SIS. We identified the following questionable activity and unnecessary permissions granted in the SIS.

- SIS accounts were logged into 81 times from systems that reside outside the United States, which could potentially indicate that those accounts have been compromised. After sharing our findings with District officials, they determined that some of the access was authorized and other access was not. Subsequent to our audit, District officials indicated that they further confirmed 80 of the 81 login events as authorized.

- Guidance counselors and guidance office secretaries made 48 final course grade changes from a failing grade to a passing grade without supporting documentation. While the grade changes were made by users that have the responsibility to change grades,

we did find 55 users without such responsibilities that have also been granted permission to change grades in the SIS.

- A keyboard specialist, whose responsibilities include looking up group permissions but not changing those permissions, made seven changes to SIS permissions. Seven other users without the responsibility to manage SIS permissions have also been granted the ability to modify group permissions in the SIS.

- The SIS has functionality that allows users to assume the account or identity of another user. We found that SIS identities were assumed over 2,000 times and SIS accounts were assumed over 200 times by 37 different users. An additional 54 users have been granted permissions to assume accounts or identities.

- 22 users are unnecessarily able to view the Social Security number field in the SIS, 21 users are unnecessarily able to view students' identification numbers, seven users are unnecessarily able to view students' medical information, 50 users are unnecessarily able to view students' order of protection information, 58 users are unnecessarily able to view students' custody information and nine users are unnecessarily able to view PPSI in the SIS audit log.

Accessing the SIS – The audit log generates a record each time a user logs into the SIS. This record includes the Internet Protocol address (IP address)[5] of the device used to login. Various ranges of IP addresses have been allocated to be used in different countries. Software and public websites are available that can further help to identify the location of systems via their IP addresses. This information can be useful in determining whether access to the SIS is appropriate. District officials should discuss with District employees any login event involving their user accounts and IP addresses of systems that reside outside the United States, as this could potentially indicate the account has been compromised.

We reviewed the SIS audit log and found 255,995 records associated with successful login between January 1, 2014 and September 25, 2015. Of these, 81 involved IP addresses of systems that reside outside the United States. These login events are associated with 15 different user accounts, 11 of which are parent accounts[6] and four of which are District employee accounts. We shared the information related to the

[5] An IP address is a numeric identifier assigned to each device, such as a computer or printer, on a network.

[6] Parent accounts are granted permissions to view information about specific students but not to modify or delete information in the SIS. Therefore, compromising one of these accounts could result in improper disclosure of student information but student records could not be inappropriately modified or deleted.

parent accounts with District officials to follow up as appropriate. The four District employee accounts are used by three teachers and one coach. One of the teacher's accounts was logged into from a system that resides in the Netherlands nine times during August 2014 and June 2015. The other two teachers' accounts were logged into from systems in Canada one and four times, respectively, during August 2014. The coach's account was logged into from a system in South Africa in July 2014. District officials do not routinely review the SIS audit log for indications of inappropriate access. Therefore, they could not take the appropriate follow-up or remediation steps to ensure the noted accounts have not been compromised.

After we shared our findings with District officials, they were able to determine that some of the access was authorized and other access was not. They indicated that passwords for the affected accounts have been changed since the instances of unauthorized access. We reviewed the log of activity in the SIS and found no evidence that information was added, modified or deleted using these accounts at the time of the noted login events. Subsequent to our audit, District officials indicated that they further confirmed 80 of the 81 login events as authorized.

Changing Grades – The official record of student grades should be accurate and preserved to ensure its integrity, as it serves as the historical record of student performance, credit accumulation, report cards and student transcripts. In addition, educators and the public evaluate school districts locally, regionally and nationally based on common student performance measures. To minimize the risk that grades will be changed inappropriately, permissions that allow for changing student grades should be restricted to those responsible for taking such action.

Over 7,800 grades were changed in the SIS between January 1, 2014 and September 25, 2015. Of those, 872 (11 percent) were changes from a failing grade to a passing grade (from 64 or below to 65 or above) and 200 of those (23 percent) were changes to students' final course grades. All but nine of the final course grade changes were changes to the minimum passing grade of 65. Teachers made 152 of the 200 final course grade changes while the remaining 48 were made by guidance counselors and guidance office secretaries. All of these employees are, to an extent, responsible for entering and changing student grades.

However, District personnel could not provide documentation to show justification and authorization for the 48 grade changes made by guidance counselors and guidance office secretaries. District personnel indicated that any change from a grade of 63 or 64 to a grade of 65 is done at the direction of the school principal per an

unwritten policy that the District does not give students 63 or 64 as a grade. This policy is the reason for 28 of the 48 changes made by guidance counselors and guidance office secretaries. According to District personnel, the remaining 20 changes were made at the request of a teacher, but there is no formal procedure followed or authorization form used when making these changes. These changes included:

- One on August 22, 2014 for the 2013-14 school year (from a 62 to a 65);
- One on September 24, 2014 for the 2013-14 school year (from a 57 to a 65);
- One on January 13, 2015 for the 2013-14 school year (from a 60 to a 100); and
- One on February 4, 2015 for the 2013-14 school year (from a 0 to a 94).

While the grade changes were made by users that have the responsibility to change grades, we found 55 users without such responsibilities that have also been granted permission to change grades in the SIS. The 55 users include:

- The Superintendent, Assistant Superintendent for Finance and Support Services, Assistant Superintendent for Instruction and Administrator;
- Six principals and two assistant principals;
- Two teachers, one of whom is also the Athletic Director and the other of whom is also interning as a principal (these teachers are able to change grades for students other than their own);
- One coach;
- Two administrative assistants and four clerical personnel; and
- Two contract counselors, one BOCES employee, 30 MORIC employees (one of whom left during our audit) and the SIS software vendor.

These unnecessary permissions increase the risk that student grades could be changed inappropriately or without authorization.

Modifying SIS Permissions – SIS access is controlled through user groups, which are programmed with permissions in the SIS based on the responsibilities of the users assigned to those groups. To minimize the risk that users will be granted unnecessary access, the ability to modify group permissions should be restricted to those responsible for managing SIS permissions.

Group permissions were modified 980 times between January 1, 2014 and September 25, 2015. All but seven of those modifications were made by MORIC personnel with the responsibility to manage permissions in the SIS. The other seven changes were made by a keyboard specialist whose responsibilities include looking up group permissions in the SIS. To prevent the inappropriate modification of group permissions, access should be limited to "view only" if modifications are not part of the employee's responsibilities.

We also identified seven other users without the responsibility to manage SIS permissions that have been granted the ability to modify group permissions in the SIS. This includes the Superintendent, the Assistant Superintendent for Instruction and five MORIC programmers. These permissions increase the risk that unauthorized or inappropriate modifications will be made to group permissions, potentially granting users more access than necessary in the SIS.

Assuming Accounts and Identities – The SIS has functionality that allows users to assume the account or identity of another user.[7] MORIC personnel indicated that this functionality is necessary for troubleshooting and access management purposes. Users do not need authorization from the assumed account owner to assume his or her account or identity, nor do they need to enter that user's password. As long as someone has permissions that allow assuming an account or identity, they can do so. Assuming an account or identity could allow an individual to view information or perform functions he or she could not with his or her own account. Therefore, to prevent inappropriate activity, only individuals who need this function to perform their job duties should be granted these permissions.

Between January 1, 2014 and September 25, 2015, SIS identities were assumed over 2,000 times and SIS accounts were assumed over 200 times. Users who assumed an account or identity include the Superintendent, the Assistant Superintendent for Instruction, the Administrator, four principals, one assistant principal, four guidance

[7] Assuming an identity allows a user to view information in the SIS for students assigned to the assumed identity. Assuming an account also allows a user to view this information, as well as perform any other activity the assumed account has permissions to perform, which could include changing grades or modifying SIS permissions.

counselors, seven clerical personnel, one aide, 16 MORIC personnel and the SIS software vendor.

We found 54 other users have also been granted permissions to assume accounts or identities. This includes:

- The Assistant Superintendent for Finance and Support Services and the Security Coordinator;
- Two principals and one assistant principal;
- Three teachers, one of whom is the Athletic Director;
- One coach;
- Two administrative assistants, three aides, eight clerical personnel and 13 substitute secretaries; and
- Two contract counselors and 17 MORIC employees (including one that left during our audit).

These powerful permissions should be strictly controlled and monitored to prevent inappropriate activity by users who would not, without such permissions, be able to perform those activities.

Viewing PPSI – The SIS also contains other PPSI about students, including student identification numbers, as well as medical, order of protection and custody information. District officials are responsible for preserving the confidentiality and integrity of this information. To prevent inappropriate access to PPSI, the ability to view this information should be restricted to those who need it to perform their job duties.

We found that numerous users have access to view PPSI unnecessarily. For example:

- 41 users have permissions to view the Social Security number field, in the SIS. Of these, 22 are unnecessarily able to view this field, including the Superintendent, the Assistant Superintendent for Instruction, a keyboard specialist, a BOCES employee and 18 MORIC employees (including programmers and technicians). Subsequent to our audit, District officials indicated that this field does not currently contain students' Social Security numbers. However, the noted permissions should be removed to reduce the risk of inappropriate disclosure if the use of this field is changed in the future.

- 67 users have permissions to view students' identification numbers. Of these, 21 are unnecessarily able to view this information, including a contract counselor, a BOCES employee and 19 MORIC employees (including programmers and technicians).

- 44 users have permissions to view students' medical information. Of these, seven users are unnecessarily able to view this information, including a keyboard specialist, five MORIC programmers and one additional MORIC employee who does not directly support the SIS for the District.

- 106 users have permissions to view students' order of protection information. Of these, 50 users are unnecessarily able to view this information, including a teacher who also serves as the Athletic Director, two administrative assistants, four aides, 12 substitute secretaries, 15 clerical personnel, one contract counselor, one BOCES employee and 14 MORIC employees (including programmers and technicians).

- 305 users have permissions to view students' custody information. Of these, 58 users are unnecessarily able to view this information, including two administrative assistants, six aides, 12 substitute secretaries, 17 clerical personnel, six contract counselors, one BOCES employee and 14 MORIC employees (including programmers and technicians).

- 30 users have permissions to view the SIS audit log which contains several items of PPSI, including passwords, home addresses, medical information and disciplinary records. Of these, nine users are unnecessarily able to view the audit log, including a keyboard specialist, seven MORIC programmers and technicians and one additional MORIC employee who does not directly support the SIS for the District.

To safeguard against inappropriate disclosure or misuse, access to students' PPSI should be minimized to those who need access to fulfill their job duties.

User Accounts

To minimize the risk of unauthorized access, user accounts in the SIS should be limited to those who currently need access to one or more functions in the SIS to perform their job duties. Access should be terminated promptly when employees leave the District or no longer need access to perform their job duties. Unnecessary user accounts increase the risk that an account could be used to inappropriately access the SIS.

We examined all 322 user accounts in the SIS as of September 25, 2015. Of these, 22 had never been used to log into the SIS and an

additional 34 had not been used to log in during the current school year. According to District personnel, 10 of the accounts never used and 16 of the accounts not used during the current school year are needed by current District or third-party personnel. Another seven and 12 accounts are for substitute secretaries and nurses who, according to District practice, should only have access to the SIS when they are substituting. Although District personnel indicated that all of these accounts are set as inactive, according to MORIC personnel, users can still log into the SIS and perform the same activities with inactive accounts as they can with active accounts.

The remaining five accounts never used are for former third-party personnel, one who left during our audit. The remaining six accounts not used during the current school year include four for former District employees, one who left the District in June 2011, and two for teachers who retired during our audit. The 11 accounts for former District and third-party personnel have the ability to perform a variety of functions in the SIS, including viewing student PPSI. One of these accounts has the ability to manage SIS accounts, assume identities and override elementary students' grades.

Figure 1: Unused User Accounts

	Never Used	Not Used During the Current School Year	Total
Current District or Third-Party Personnel	10	16	26
Current Substitute Secretaries or Nurse	7	12	19
Former Third-Party Personnel	5[a]	0	5
Former District Employees	0	6[b]	6
Total	**22**	**34**	**56**

[a] One of these users left during our audit.
[b] Two of these users left during our audit.

We identified another three user accounts created for substitute secretaries and nurses, and two additional accounts created for MORIC personnel who do not provide direct support to the District for the SIS. Substitutes should only have access to the SIS when they are substituting and MORIC personnel should only have the access necessary for the support they provide to the District.

These unnecessary accounts increase the risk that an account could be used to inappropriately access the SIS. It also increases the efforts needed to manage permissions in the SIS, increasing the risk of errors that inadvertently grant more access than needed.

Management and Monitoring

The Administrator, with support from other District and MORIC employees, is responsible for protecting and preventing improper access to PPSI. To fulfill these responsibilities, the Administrator should monitor audit logs for indications of inappropriate activity. To guide these efforts, the Board should develop comprehensive written

policies and procedures for reviewing SIS audit logs and managing SIS accounts and permissions.

District officials do not review the SIS audit logs on a regular basis nor do they properly manage SIS accounts and permissions. In addition, they have not established effective policies and procedures for protecting PPSI in the SIS. The questionable activity, unnecessary permissions and unnecessary user accounts we identified were the result of, at least in part, District officials' failure to properly manage and monitor access to the SIS.

Reviewing Audit Logs – Audit logs maintain a record of activity in a computer application. District officials should review these logs to monitor for indications of inappropriate activity. However, District officials have not established a process for reviewing audit logs on a regular basis. Because we found that users are assigned more permissions than needed for their job duties, it is even more important that District officials monitor user activities to help detect inappropriate use of the SIS. By not conducting these reviews, District officials were unaware of the activities previously identified in this report and, therefore, could not take the appropriate follow-up or remediation steps.

Managing Accounts and Permissions – District officials should properly manage accounts and permissions to ensure access to the SIS is limited to those with a business need and users have the least amount of access necessary to perform their job duties. The Administrator, with support from other District and MORIC employees, is responsible for adding and removing accounts and permissions in the SIS. According to District personnel, SIS users and permissions are reviewed throughout the school year. However, they told us that user accounts for personnel who are terminated or leave the District may not be removed in a timely manner if personnel are busy. Both District and MORIC personnel also told us that they are unsure of the meaning of the permissions available and assigned in the SIS. These weaknesses resulted in the unnecessary permissions and user accounts.

Establishing Policies and Procedures – The District should have comprehensive written policies and procedures for protecting the PPSI in the SIS. However, District officials have not established a policy regarding what information should be available in the SIS or how that information should be safeguarded. Furthermore, District officials have not established procedures for monitoring activity in the SIS. While procedures and guidelines have been established for authorizing new SIS user accounts and assigning permissions to those accounts, these are not effective in ensuring users are not assigned more permissions than necessary. Finally, procedures for

reviewing user accounts and permissions are informal and ineffective. Without proper policies and procedures, District and MORIC personnel may not understand their roles and responsibilities, or District officials' expectations, for granting and restricting access to the SIS. The findings described throughout this report result, at least in part, from the lack of effective policies and procedures.

Recommendations

The Board should:

1. Require documentation to be retained to show who authorized grade changes and the reasons for the changes.

2. Establish written policies and procedures for managing and monitoring access to the SIS. This should include requirements for safeguarding PPSI and procedures for monitoring user activity.

The Administrator should:

3. Review IP address information available in the SIS audit log for activity indicative of potential compromise.

4. Restrict the ability to modify SIS permissions to designated individuals and periodically review modifications for appropriateness.

5. Strictly control the ability to assume identities and accounts to designated individuals and monitor activity associated with these functions.

6. Evaluate permissions currently granted to each SIS user, including MORIC employees and vendors, and remove any permissions deemed unnecessary.

7. Evaluate all existing SIS user accounts and remove any accounts deemed unnecessary.

8. Periodically review SIS audit logs for unauthorized or inappropriate activity.

9. Ensure that SIS user accounts for personnel that are terminated or leave the District are removed timely.

10. Work with the software vendor to gain a better understanding of the available SIS permissions. Work with MORIC personnel to thoroughly test the permissions currently assigned to SIS users.

11. Review current procedures for assigning and monitoring SIS permissions and strengthen controls to ensure that individuals are assigned only those permissions needed to perform their job duties.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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

ONEIDA CITY SCHOOL DISTRICT
565 Sayles Street, Post Office Box 327, Oneida, New York 13421 · Phone (315) 363-2550 · Fax (315) 363-6728
http://www.oneidacsd.org

- RONALD R. SPADAFORA JR., Superintendent of Schools
- JAMES J. ROWLEY, Assistant Superintendent for Finance
- BRIAN D. KAVANAGH, Assistant Superintendent for Instruction

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

Audit Response

Unit Name: Oneida City School District
Audit Report Title: Controlling Access to the Student Information System
Audit Report Number: 2016-M-58
Attention: Office of the Comptroller

Please accept this letter as the written audit response of the Oneida City School District to your draft report of examination letter dated April 2016. After receiving and reviewing your final report, we will prepare a Corrective Action Plan and submit it as required. Some of the recommendations made in the Draft Report have already been implemented, and these will be identified further in the Corrective Action Plan.

We understand the Office of the State Comptroller conducted audits 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 our District has provided us with an opportunity to examine our procedures and identify areas for improvement.

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). Our Board Policy No. 7061.1 concerning Student Records has long guided the District's compliance with FERPA. The recommendations in your Draft Report will assist us in our continuing efforts to comply with federal law and Board policy.

With respect to the Comptroller's opinion, we note the examination did not identify any circumstance constituting a violation of any state or federal statute or regulation. Nor does the Draft Report identify any instance of inaccurate or fraudulent data alteration.

The Oneida City School District respects the importance of adequately safeguarding personal, private, sensitive information (PPSI) in the SIS and therefore feel it is imperative to clarify a few statements mentioned in the Draft Report. Responses to the remaining items mentioned in the Draft Report will be forthcoming in the Corrective Action Plan.

- *Draft Report: "SIS accounts were logged into 81 times from systems that reside outside the United States, which could potentially indicate that those accounts have been compromised.*

After sharing our findings with District officials, they determined that some of the access was authorized and other access was not."

- District Response: The District has knowledge of employees that travel to countries outside of the United States throughout the school year, over school breaks, and over the summer. In addition to staff travel, students' parents travel for work and/or are deployed to other countries outside of the United States. 80 of the logged accounts in the report have been confirmed. 1 account noted in the report is of a former employee of the district and has not been confirmed.

See Note 1 Page 21

- *Draft Report: "A keyboard specialist, whose responsibilities include looking up group permissions but not changing those permissions, made seven changes to SIS permissions."*
  - District Response: The keyboard specialist in question works as the District Data Specialist in conjunction with the District Data Coordinator. This staff member was hired in a keyboard specialist civil service title. Any changes for permissions are made in conjunction with the Administrator for Technology and Special Programs/ District Data Coordinator. The District agrees with the Comptroller's opinion to retain a paper trail of changed permissions and has taken corrective action.
- *Draft Report: "22 users are unnecessarily able to view students' Social Security numbers"*
  - District Response: The SIS is not used to collect nor does it contain Social Security numbers. The numbers in those fields are random numbers ranging from 0-4,444. The Social Security Number field in the SIS was used as temporary storage for numbers that provided background data linkages during the district's implementation of [redacted] in 2007. These numbers are not valid Social Security Numbers.

See Note 2 Page 21

- *Draft Report: "The questionable activity, unnecessary permissions and unnecessary user accounts we identified result, at least in part, from the lack of effective management and monitoring of access to the SIS."*
  - District Response: The District provides SIS accounts and permissions with sign off documentation based on the specific user's job duties. Duties regularly change for employees depending on instructional and support assignments. These job duties are determined by district office personnel and signed off by the Administrator for Technology and Special Programs.

See Note 3 Page 21

- *Draft Report: "These unnecessary [user] accounts increase the risk that an account could be used to inappropriately access the SIS. It also increases the efforts needed to manage permissions in the SIS which could allow inadvertently granting more access than needed."*
  - District Response: The unnecessary user accounts are all deactivated accounts in both Active Directory and SIS. Accounts remain deactivated in lieu of being deleted for audit history. Deactivated accounts cannot log into the network or the SIS. As an additional precaution, the District will remove the deactivated users from groups as well. All accounts deemed unnecessary by the district have since been removed from their former [redacted].

See Note 4 Page 21

- *Draft Report: "District officials do not review SIS audit logs on a regular basis nor do they properly manage SIS accounts and permissions."*
  - District Response: SIS accounts and permissions are reviewed in conjunction with the MORIC. Any changes in personnel who are terminated or leave the district are reviewed and acted upon.

See Note 3 Page 21

The District 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 understands the over-arching 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 enhanced compliance.

To date, the district has started a corrective action in the areas of recommendation listed in the Draft Report. We continue to work with our technology partners at the MORIC to refine any policies and procedures pertaining to the SIS. These items will be expanded upon in our forthcoming Corrective Action Plan.

Sincerely,

Robert Group
Board of Education President

APPENDIX B

OSC COMMENTS ON THE DISTRICT'S RESPONSE

Note 1

We modified our report to acknowledge that, subsequent to our audit, District officials indicated that they confirmed 80 of the 81 login events as authorized. Going forward, the Administrator should perform periodic reviews of the SIS audit log for similar activity to detect inappropriate access and allow timely remediation whenever necessary.

Note 2

We modified our report to acknowledge that, subsequent to our audit, District officials indicated that the Social Security number field does not currently contain students' Social Security numbers. However, the noted permissions should be removed to reduce the risk of inappropriate disclosure if the use of this field is changed in the future.

Note 3

We commend District officials for having a process in place to create SIS accounts, assign SIS permissions and review accounts and permissions with MORIC personnel. However, the unnecessary permissions and accounts identified during our audit demonstrate that District officials could improve this process to strengthen controls over SIS access.

Note 4

All unnecessary accounts noted in this report were active in both Active Directory and the SIS at the time of our testing. We commend District officials for taking timely action to deactivate these accounts.

APPENDIX C

AUDIT METHODOLOGY AND STANDARDS

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

- We interviewed District and MORIC personnel to obtain an understanding of the District's SIS and related IT access controls.

- We compared a list of active District employees to a list of current SIS users to determine if any SIS users are not District employees or if any former employees remained on the user list. For all users that are not current or former District employees, we interviewed District and MORIC personnel to determine if those users provide technical or other support that requires access to the SIS.

- For all users with last login dates prior to the start of the current school year, we interviewed District officials to determine if those users have a current, legitimate business need to access the SIS.

- We compared all users' job roles with user group assignments to determine if high-risk permissions[8] are compatible with responsibilities. For each user with one or more group assignments different than users with the same job role (e.g., a teacher who also has permissions of a principal, or a secretary who also has permissions of a SIS administrator), we interviewed District officials to determine if the user has responsibilities that require the additional permissions.

- We analyzed the audit logs generated by the District's SIS to identify those that come from IP addresses outside the United States and to determine if student grades were changed, group permissions were modified, or accounts or identities were assumed inappropriately or without authorization.

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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

[8] We defined high-risk permissions as those that allow managing user accounts, granting and changing SIS access, assuming accounts and identities, viewing the SIS audit log, changing grades and viewing students' Social Security numbers, identification numbers, medical information, order of protection information and custody information.

APPENDIX D

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller
Public Information Office
110 State Street, 15th Floor
Albany, New York 12236
(518) 474-4015
http://www.osc.state.ny.us/localgov/

APPENDIX E

OFFICE OF THE STATE COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY

Andrew A. SanFilippo, Executive Deputy Comptroller
Gabriel F. Deyo, Deputy Comptroller
Tracey Hitchen Boyd, Assistant Comptroller

LOCAL REGIONAL OFFICE LISTING

BINGHAMTON REGIONAL OFFICE
H. Todd Eames, Chief Examiner
Office of the State Comptroller
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313
Email: Muni-Binghamton@osc.state.ny.us

Serving: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins Counties

BUFFALO REGIONAL OFFICE
Jeffrey D. Mazula, Chief Examiner
Office of the State Comptroller
295 Main Street, Suite 1032
Buffalo, New York 14203-2510
(716) 847-3647 Fax (716) 847-3643
Email: Muni-Buffalo@osc.state.ny.us

Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming Counties

GLENS FALLS REGIONAL OFFICE
Jeffrey P. Leonard, Chief Examiner
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, New York 12801-4396
(518) 793-0057 Fax (518) 793-5797
Email: Muni-GlensFalls@osc.state.ny.us

Serving: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington Counties

HAUPPAUGE REGIONAL OFFICE
Ira McCracken, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788-5533
(631) 952-6534 Fax (631) 952-6530
Email: Muni-Hauppauge@osc.state.ny.us

Serving: Nassau and Suffolk Counties

NEWBURGH REGIONAL OFFICE
Tenneh Blamah, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725
(845) 567-0858 Fax (845) 567-0080
Email: Muni-Newburgh@osc.state.ny.us

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester Counties

ROCHESTER REGIONAL OFFICE
Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street, Suite 522
Rochester, New York 14614-1608
(585) 454-2460 Fax (585) 454-3545
Email: Muni-Rochester@osc.state.ny.us

Serving: Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates Counties

SYRACUSE REGIONAL OFFICE
Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428
(315) 428-4192 Fax (315) 426-2119
Email: Muni-Syracuse@osc.state.ny.us

Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence Counties

STATEWIDE AUDITS
Ann C. Singer, Chief Examiner
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313