OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY

Access Controls Over Student Information Systems

2014-MR-1

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

August 2014

Dear District Officials:

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 school district operations. The Comptroller oversees the fiscal affairs of school 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 school district operations and Board of Education governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard school district assets.

Following is a report of our audit titled Access Controls Over Student Information Systems. 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 General Municipal Law.

This audit's results and recommendations are resources for school 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

School districts maintain and use student personal information for a variety of educational purposes. School districts use software applications, often referred to as Student Information Systems (SIS), to store and manage student data in a centralized database. These systems include a considerable amount of personal, private and sensitive information (PPSI),[1] which students and their parents entrust school district officials to safeguard. Access to PPSI in the SIS should be limited to only those with a business need (i.e., operations, instruction, management and evaluation) and users should have the least amount of access necessary to perform their job duties or responsibilities.

The six districts included in this audit – Altmar-Parish-Williamstown (APW) Central School District, Indian River Central School District, Lowville Academy and Central School District, Madison Central School District, Poland Central School District and Westhill Central School District – maintained PPSI for a total of 9,730 students in 2011-12.

Scope and Objective

The objective of our audit was to review access to SIS data for the period July 1, 2011 through April 30, 2013. We extended our scope period through November 12, 2013 to perform certain tests of the districts' access controls. Our audit addressed the following related question:

- Did the districts adequately control access to SIS?

Audit Results

The districts that we reviewed did not adequately control access to SIS. As a result of control weaknesses at each district, we found that certain users in all six districts were assigned more access rights than needed for their job duties.

We tested 229 users from a total of 1,909 users[2] (12 percent) in all six districts and compared the users' SIS permissions to their job duties and responsibilities. We found that 90 users (39 percent)

[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] Of the 5,507 total combined district SIS users, 3,598 are parent and student users. We found that parent and student access rights were appropriate. Our testing focused on the remaining 1,909 users (i.e., staff, Regional Information Center (RIC) employees and vendors). The 1,909 users include 45 RIC employees who provide SIS support at more than one district, and they are included as users at each of these districts.

had access to one or more functions even though it was not their job responsibility to perform these functions.[3] We found that 13 of these users performed functions that were not required by their job duties. For example, two users from Madison made 141 grade changes even though it was not their responsibility to change grades. We tested 70 grade changes[4] from districts' audit logs and found that the documentation supporting the grade changes was either not complete or not retained due to the lack of a formal process for documenting grade changes. At Madison and Indian River, grade changes made by unauthorized users and without supporting documentation included changes from 47 to 70, 58 to 70 and 62 to 70. Further, at Indian River, 19 of 40 grade changes were made by a Mohawk Regional Information Center employee who was not assigned the responsibility to change grades and there was no documentation to support these grade changes. When the ability to change grades is not properly restricted and there is no process to require that all changes be authorized, supported and documented, there is an increased risk that unauthorized or inappropriate changes can be made to grades without detection.

None of the districts had adopted written policies and procedures for adding users, establishing users' access rights, deactivating or modifying user accounts and monitoring user access. Also, none of the districts had an effective process in place for adding and changing user rights, and none of the districts, except APW, periodically evaluated and monitored user rights once rights had been assigned to ensure that the rights remained current and appropriate. We found that attendance records were changed 185 times at Indian River and 31 times at Lowville using a former employee's user account. Officials told us that former employees' user names and passwords were shared with other employees so they could update the SIS after the employees left district employment. We also found that a generic user account was used to view a student's Individualized Education Program (IEP) at Indian River. Officials do not know who accessed the IEP because the account was not assigned to a specific individual.

Our testing also found that four of the six districts (Indian River, Lowville, Madison and Poland) have features within SIS that allow users to assume the identity or the account of another user. The assume-identity feature allows a user to access student information for those students assigned to the user whose identity was assumed. The assume-account feature allows a user to assume the account of another user and inherit all the given rights and permissions of that user. We found that 39 users in our sample of 144 have the ability to use the assume-identity feature and 31 users have the ability to use the assume-account feature. The use of these features makes it difficult for district management to know who is making changes or viewing information.

In addition, management at three of the districts (Westhill, Madison and Poland) do not authorize assigned user rights, and none of the districts reviewed audit logs or change reports for potentially unauthorized changes. Because we found that users at all the districts were assigned more rights

[3] In the five districts that utilize user groups to assign access rights, we found that the user groups that the individuals were assigned to included numerous other users with permissions that were not required for their jobs. At APW, we searched electronic user access reports for particular permissions (e.g., the ability to change grades) and identified a number of additional users who also had more rights than needed.

[4] Our test included 40 grade changes in Indian River and 10 changes each in Lowville, Madison and Poland. The 10 grade changes we reviewed in Madison were a sample of the 141 changes made by unauthorized users that we previously identified.

than needed for their job duties, it is even more important that the districts monitor user activities to help detect improper access to PPSI in the SIS. When audit logs or change reports are not generated and reviewed, officials cannot be assured that unauthorized activities, such as improper grade changes, are detected and adequately addressed.

Our audit disclosed areas where additional information technology security controls and measures should be instituted. Because of the sensitive nature of some 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.

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.

Introduction

Background

School districts maintain and use students' personal information for a variety of educational purposes. School districts use software applications, often referred to as Student Information Systems (SIS), to store and manage student data in a centralized database. SIS commonly contain extensive information about students, including parent and emergency contacts, attendance, disciplinary actions, testing, schedules, grades and medical information. Therefore, these systems include a considerable amount of personal, private and sensitive information (PPSI),[5] which students and their parents entrust school districts to safeguard. School districts provide SIS access to teachers, administrators, various staff members and external information technology (IT) support staff. In addition, many school districts provide parents with limited access to their children's information and also provide students with limited access to their own information. Access to PPSI should be limited to only those with a business need (i.e., operations, instruction, management and evaluation) and users should have the least amount of access necessary in order to perform their job duties or responsibilities.

We audited six districts located in central and northern New York State. Each district has a manager who is responsible for directing day-to-day SIS operations. All six districts receive technical support from a Regional Information Center (RIC)[6] and provide their respective RIC or vendor with SIS access to perform this function. In addition, all six districts provide parent access and two districts[7] provide student access.

[5] 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.

[6] There are 12 RICs in the State, each administratively aligned under a Board of Cooperative Educational Services (BOCES). The RICs provide participating school districts and BOCES with a variety of technology services.

[7] Indian River and Westhill

Table 1: District Information

School District	2011-12 Student Enrollment	SIS RIC Support[a]	No. of SIS Users	No. of User Groups/ Roles	SIS Manager
Altmar-Parish-Williamstown (APW)	1,300	CNYRIC	504	30	Network Administrator
Indian River	4,100	MORIC	1,766	20	Assistant Superintendent of Curriculum and Instruction
Lowville Academy	1,390	MORIC	666	21	Instructional Technology Specialist and Computer Network Manager
Madison	470	MORIC	311	18	Technology Coordinator
Poland	620	MORIC	294	23	Guidance Secretary
Westhill	1,850	WNYRIC and CNYRIC	1,966	29	Director of Technology

[a] Central New York RIC (CNYRIC), Mohawk RIC (MORIC) and Western New York RIC (WNYRIC) provide SIS support. Westhill receives SIS support from WNYRIC and stores its SIS data at the CNYRIC, Lowville stores SIS data in-house at the district and the other four districts store SIS data at their respective RICs.

Objective

The objective of our audit was to review access to SIS data. Our audit addressed the following related question:

- Did the districts adequately control access to SIS?

Scope and Methodology

For the period July 1, 2011 through April 30, 2013, we interviewed district officials and staff and examined policies and procedures to control and monitor access to each district's SIS. We extended our scope period through November 12, 2013 to perform certain tests of the districts' access controls. Our audit disclosed areas where additional IT security controls and measures should be instituted. Because of the sensitive nature of these findings, certain vulnerabilities are not discussed in this report but have been communicated confidentially to district officials so they could take corrective action.

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.

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.

Access to Student Information Systems

Parents and students rely on district officials to ensure that students' personal information is properly safeguarded. District officials are responsible for protecting and preventing improper access to PPSI in SIS. To fulfill these responsibilities, district officials should develop comprehensive written user access policies and procedures designed to protect and monitor access to PPSI. Management should verify assigned user rights, periodically monitor user rights to ensure they are current and appropriate and periodically monitor change reports or audit logs for any unusual activity to help ensure that only appropriate changes are being made by authorized users.

The districts that we reviewed did not adequately control access to SIS. None of the districts adopted comprehensive user access policies and procedures, increasing the risk that PPSI could be accessed, changed or misused by unauthorized persons. Our tests of 229 SIS users found that 90 users (39 percent) had access to one or more functions even though it was not their job responsibility to perform those functions. We also found that none of the districts reviewed audit logs or change reports for potentially unauthorized changes. When audit logs or change reports are not generated and reviewed, officials cannot be assured that unauthorized activities, such as improper grade changes, are detected and adequately addressed.

Policies and Procedures

District officials should develop comprehensive written policies and procedures for protecting PPSI from unauthorized use or modification. Essential measures include restricting access to authorized users and restricting users' access to only those functions and data that are necessary for the users' day-to-day duties and responsibilities. Further, policies should establish controls over users' access to SIS, including adding users, establishing access rights and deactivating or modifying user accounts, as well as the process that will be used to monitor access.

All six districts have policies limiting access to only authorized district personnel and breach notification policies that detail how district employees would notify affected parties whose private information was, or is reasonably believed to have been, acquired without valid authorization. However, none of the districts adopted comprehensive written policies and procedures addressing user

access issues such as adding, deactivating or modifying user rights and accounts.

As a result of control weaknesses at each district, we found that certain users were assigned more rights than needed for their job duties. Without written procedures for staff responsible for the maintenance of user accounts and monitoring access rights, there is an increased risk that rights will be assigned incorrectly and that access to SIS will not be properly restricted.

User Access

District officials should ensure that there are written procedures in place for granting, changing and terminating access rights to SIS. These procedures should establish who has the authority to grant or change access (e.g., supervisory approval). Also, it is important to limit individual user access rights within the SIS to only those functions necessary to fulfill individual job responsibilities. Such controls limit the risk that sensitive or confidential information will be exposed to unauthorized use or modification.

All the districts, except APW, assign SIS access rights by user group. Each user group has an associated set of rights and permissions and once a user is added to a group, that user has the same rights and permissions to view or modify data as all the other users in the group. If a user needs rights different than those in any established user group, a new user group can be created for the user, or, in some cases, the user can be assigned to multiple groups that provide different levels of access.[8] The five districts have each established between 18 to 29 different user groups to assign access rights. APW assigns users to one of 30 user roles with associated user rights and permissions. Unlike the groups in the other districts, once a user is assigned a role, APW can customize the rights for each user by adding or removing rights in each individual user account.

To determine if user access at each district is compatible and appropriate, we identified SIS users responsible for performing certain functions at the districts, such as changing grades, viewing and modifying health records, changing student demographic information[9] and adding staff user accounts. We tested a sample

[8] Westhill users can only be assigned to one SIS user group. Indian River, Lowville, Madison and Poland users may be assigned to multiple user groups.

[9] Such as student age, student user identification number, address and parent contact information

of 229 users from a total of 1,909 users[10] (12 percent) in the six districts and compared the users' SIS permissions to the users' job duties and responsibilities. We found that 90 users (39 percent) had access to one or more functions for which it was not their job responsibility to perform these functions.

Table 2: Test of User Access Rights

School District	Users Tested	Users With More Access Rights than Needed for Their Jobs[a]	Percentage of Users With More Access Rights than Needed
APW	35	8	23%
Indian River	60	20	33%
Lowville	34	15	44%
Madison	21	13	62%
Poland	29	13	45%
Westhill	50	21	42%
Total	**229**	**90**	**39%**

[a] Users were provided with access rights such as the ability to change student grades, view and modify student health records, change student demographic information or add new staff user accounts.

In the five districts that assign access rights by user group, those user groups included numerous users with permissions that were not required for their jobs. In APW, we searched electronic user access reports for particular permissions (e.g., the ability to change grades) and identified a number of additional users who had more rights than needed. Table 3 shows the number of users designated by the districts as responsible for performing certain SIS functions and those who also have access to perform those functions even though it is not their responsibility to do so.[11]

[10] Of the 5,507 total combined district SIS users, 3,598 are parent and student users. We found that parent and student access rights were appropriate. Our testing focused on the remaining 1,909 users (i.e., staff, RIC employees and vendors). The 1,909 users includes 45 RIC employees who provide SIS support at more than one district, and they are included as users at each of these districts.

[11] See Appendix C for details by district.

Table 3: Users With Access to Certain SIS Functions

Function	Total Number of Users Designated to Perform Each Function	Additional Number of Non-Designated Users With Access to Perform Each Function[a]			
		RIC Staff[c]	District Staff	SIS Vendor[c]	Total
Grade Changes	129	153	105	4	**262**
View/Modify Health Records[b]	68	101	7	2	**110**
Change Student Demographic Information	111	151	186	4	**341**
Add Staff User Account	92	132	101	4	**237**

[a] Some users had multiple user rights that were not necessary given their job duties and these users are included in more than one SIS function.
[b] This function was not assessed at Madison and Lowville because neither district uses SIS to store student medical records.
[c] The total RIC Staff for each function includes technical staff who provide SIS support at more than one of the districts. The total SIS Vendor staff for each function is the same vendor user at four of the districts.

Users' accounts with unnecessary access rights were assigned to district staff, RIC staff and the SIS vendor. RIC officials told us that their SIS support staff require full access rights in order to assist districts with day-to-day troubleshooting. We did not include SIS support staff as exceptions in our testing. However, we did include the SIS vendor and other RIC technical staff (i.e., programmers and technicians) as exceptions because they were granted full SIS access rights and they only need occasional access for troubleshooting.

District staff responsible for granting user access at Westhill were unsure of the meaning of the rights and permissions within each staff user group. For example, they did not know the meaning of group access rights classified under titles such as "access accounts," "historical grades" and "functions." Similarly, staff at Indian River do not have lists of the rights granted to each user group to verify that access needs are compatible with the rights of the assigned groups. Four districts (Indian River, Lowville, Madison and Westhill) assign user rights based on a historic knowledge of prior users who were assigned the same role. Assigning the same rights to a new user as the predecessor in the same job title/role does not guarantee that the user rights assigned are accurate. In addition, management at three of the districts (Westhill, Madison and Poland) does not authorize the assigned user rights. At these districts, the responsibility for authorizing user rights is given to district staff[12] who are also responsible for adding, deactivating and modifying user accounts and rights without supervisory or management review. This increases the risk that more access rights than necessary may be assigned to users. While officials at

[12] District Office Secretary/Board Clerk at Westhill and SIS Managers at Madison and Poland

APW reviewed non-instructional staff user rights and permissions for appropriateness during the 2011-12 fiscal year and removed unneeded rights from the users' accounts at that time, none of the other districts periodically evaluated and monitored user rights once rights were assigned to ensure that the rights are current and appropriate. Because a significant number of users have more access rights in the SIS than district officials realized or intended, there is an increased risk that sensitive or confidential student information could be compromised.

Given the significant number of users who have unnecessary access rights in each district's SIS, we requested audit logs[13] to review user activity and determine if any unauthorized changes were made by the users in our initial sample (see Table 2). Four districts provided audit logs for our review, but APW and Westhill were unable to provide usable logs (see Report Monitoring section). Our review of the usable audit logs for the 61 unauthorized users found that 13 users performed functions that were not required by their job duties, as follows:

- Two users from Madison (the guidance counselor and an office assistant/teacher aide) made 141 grade changes even though it was not their responsibility to change grades.

- Eight unauthorized users among four districts made 190 changes to student demographic information (149 changes at Lowville, 28 changes at Indian River, 10 changes at Madison and three changes at Poland).

- Three users in Lowville added new staff user accounts, even though it is not their responsibility to do so.

We also reviewed a sample of 70 grade changes[14] from the four districts' audit logs to determine if the grade changes were authorized, documented and supported. We found that the documentation supporting the grade changes was either not complete or not retained. For example:

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

[14] Our test included 40 grade changes in Indian River and 10 changes each in Lowville, Madison and Poland. The 10 grade changes we reviewed in Madison were a sample of the 141 changes made by unauthorized users that we previously identified.

- Lowville was able to provide documentation for the 10 grade changes we tested and all the changes we reviewed were made by an authorized user. However, the documentation retained did not show authorization for the changes and the reason for the changes.

- District officials at Indian River, Madison and Poland provided verbal explanations for the other 60 grade changes we tested, but they had no formal process for documenting grade changes, including who authorized the changes, the reason for the changes and the documentation to be retained. Grade changes we identified that were made by unauthorized users and without adequate supporting documentation in Madison and Indian River included changes from 47 to 70, 58 to 70 and 62 to 70.

- At Indian River, 19 of the 40 changes were made by a MORIC employee who worked onsite at the District but was not assigned the responsibility to change grades. The MORIC employee told us that teachers provided verbal and written lists of grade changes to be made, but she shredded the lists after completing the grade changes.

When the ability to change grades is not properly restricted and there is no process to require that all changes be authorized, supported and documented, there is an increased risk that unauthorized or inappropriate changes can be made to grades without detection.

User Accounts

Effective access controls require that SIS user accounts be linked to specific individuals to help prevent and detect unauthorized activity. Users should not be allowed to share user accounts and generic accounts[15] should generally not be permitted. Also, access should be terminated promptly when employees leave the district.

We compared lists of each district's active employees to lists of current staff SIS users to determine if any SIS users were not current district employees. We found 63 unknown and generic user accounts that were not assigned to any one individual, 44 active user accounts assigned to employees who no longer worked for the districts and 14 shared accounts. We reviewed the usable audit logs at four districts to determine if any changes were made

[15] Generic user accounts are not assigned to a specific individual and are typically used by multiple users.

by the 47 unknown/generic, shared or former employee user accounts identified in those districts.[16] We found activity in three of the 47 accounts we tested. Specifically, 216 changes were made to update attendance records using two former employee user accounts after the employees left Indian River and Lowville (185 changes at Indian River and 31 changes at Lowville). Officials from both districts told us that the former employees' user names and passwords were shared with other employees so they could update SIS after the employees left district employment. We also found a generic user account was used to view a student's Individualized Education Program (IEP) at Indian River. Because this account was not assigned to a specific individual, Indian River officials did not know who accessed the IEP. When generic and shared accounts are used, accountability is diminished and activity in the system may not be able to be traced back to a single user. Furthermore, if individuals who are no longer active employees have SIS access rights, they may inappropriately obtain confidential data, and there is an increased risk that they can use the system for improper purposes.

Our testing also found that four of the six districts (Indian River, Lowville, Madison and Poland) have features within SIS that allow users to assume the identity or the account of another user. The assume-identity feature allows a user to access student information for those students assigned to the user whose identity was assumed. The assume-account feature is even more powerful in that it allows a user to assume the account of another user and also inherit all the given rights and permissions of that user. Officials from MORIC, which supports SIS at these four districts, said that certain MORIC employees use the assume-identity/account features for troubleshooting when the districts need assistance. However, a large number of other district staff and MORIC employees were given this capability, even though they were not involved in day-to-day troubleshooting. We found that 39 users in our sample of 144[17] have the ability to use the assume-identity feature and 31 users have the ability to use the assume-account feature. Because user rights and permissions are the same for all users within each user group at these four districts, we determined that 194 users can use the assume-identity feature and 175 users can use the assume-account feature. These users do not need this function for their routine job duties, so they should not

[16] We were not able to test the 74 inappropriate user accounts found in APW and Westhill because usable audit logs were not available.

[17] 229 users sampled, less 85 users in Westhill and APW whose SIS does not include the assume-identity/account feature, equals 144 users.

be granted this capability.[18] Furthermore, the audit logs for these districts do not show the user whose identity or account has been assumed, and they do not clearly differentiate what actions were completed under an assumed identity or account. This makes it difficult for management to evaluate how often these powerful features are used and whether they are used to make changes or view information by individuals that would otherwise not have access through their own user account.

Report Monitoring

Audit logs or change reports[19] 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. None of the districts we reviewed monitor audit logs or change reports.

Indian River, Lowville, Madison and Poland are able to produce audit logs, but those districts did not generate audit logs or review them for potentially unauthorized changes. Officials at APW and Westhill were initially not aware if any audit logs or change reports could be generated from their systems. Officials at both these districts attempted to generate reports upon our request during fieldwork, but the reports generated were not useful as they were complex and did not clearly show user activity.

Because we found that users at all six districts were assigned more rights than needed for their job duties, it is even more important that these districts monitor user activities to help detect improper SIS access to PPSI. When audit logs or change reports are not generated and reviewed, officials cannot be assured that unauthorized activities, such as improper grade changes, are detected and adequately addressed.

Recommendations

District officials should:

1. Establish written policies and procedures for SIS administration including a formal authorization process to add, deactivate or change user accounts and rights and procedures for monitoring user access,

[18] See Appendix C for details by district. We did not include MORIC SIS support staff members who are involved in day-to-day troubleshooting as exceptions in our testing. However, we did include MORIC technical staff (i.e., programmers and technicians) and the vendor as exceptions because they rarely need this type of access to the SIS.

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

2. 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 and should monitor user access rights periodically,

3. Evaluate user rights and permissions currently assigned to each SIS user, including RIC employees and vendors, and ensure that rights are updated as needed to properly restrict access,

4. Restrict the ability to make grade changes to designated individuals and ensure that documentation is retained to show who authorized the grade changes and the reasons for the changes,

5. Remove all unknown and generic or shared SIS accounts and deactivate the accounts of any users who are no longer employed,

6. Determine whether the assume-identity and assume-account features are appropriate for use (if currently available); if these features are used, district officials must strictly control access and review SIS data that clearly shows user activity performed and all accounts involved when these features are used, and

7. Periodically review available audit logs for unusual or inappropriate activity. If useful audit logs are currently not available, District officials should work with their SIS provider to determine if useful logs or change reports can be generated to monitor activities.

APPENDIX A

RESPONSES FROM DISTRICT OFFICIALS

We provided a draft copy of this global report to the six districts we audited and requested responses. We received a response letter from five districts. We also provided a draft version of the respective individual letter reports to each of the six districts. We received responses from six districts. The districts generally agreed with our audit report; however, one of the districts had comments that we respond to within this Appendix.

Overall Comments

Altmar-Parish-Williamstown Central School District officials said: "The draft audit report was enlightening and appropriate, APW administration and staff very much appreciate the time and energy that OSC spent reviewing internal controls of the student management system. The results of this finding specific to APW will be incorporated into a policy and procedures document that will guide further work in this area."

Indian River Central School District officials said: "The District is in agreement with the findings of the audit that pertain to Indian River. The District is in the process of developing and documenting interventions that address the recommendations detailed in the report. We have initiated collaboration to address specific recommendations contained in the report with the Regional Information Center (MORIC)."

Lowville Academy and Central School District officials said: "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." "While some discrepancies were identified, the Mohawk Regional Information Center has provided assistance and direction in resolving these discrepancies."

Poland Central School District officials said:

"The District has reviewed current procedures for assigning user access rights and has strengthened controls to ensure that individuals are assigned only to rights needed to perform job duties and functions."

"The District is working with the MORIC to identify the pathway of rights granted to each user group. As permissions are evaluated, eliminating the access to additional or unnecessary rights to any user will be remedied."

"The District has removed unknown accounts that had once been created for ease of functioning and off-campus support. Staff members who require SIS access have been given direct access specific to their needs."

"The District has identified key personnel who will be authorized to make grade changes through SIS and has restricted access to the grade change function. The District has initiated a paperwork

trail for grade changes....Written documentation specific to the need for the grade change will be maintained."

"The District has limited both "assume" functions. The District is working with the SIS to determine if the audit log can accurately capture user activity in the "assume" setting."

"The District will work with the MORIC to access and review audit logs to help identify unusual or inappropriate activity and increase checks and balances."

Westhill Central School District officials said:

"On May 20, 2014, the district updated Policy 7240, Student Records: Access and Challenge. In addition, the district has updated administrative regulations for adding, deactivating, or changing user accounts and/or rights."

"With the assistance of the Western New York Regional Information Center (WNYRIC), permissions for all existing users were reset to their particular group and a current process is in place to compare access rights at different points in time to identify discrepancies."

"The district has requested that the WNYRIC work collaboratively with the vendor to develop a comprehensive security report to allow the district to evaluate user rights and permissions for each SIS user."

"With assistance of the WNYRIC, the district has reset the permissions for all SIS users and made all unknown or unassigned accounts inactive."

"The district has requested that the WNYRIC work collaboratively with the vendor to develop a usable audit log to allow the district to review change reports, including prior years."

"Grade changes will be reviewed and approved by the respective administrator and documentation retained."

Grade Change Documentation

Madison Central School District officials said: "We are aware of no regulations or guidance issued by the State Education Department mandating any particular form of documentation for grade changes, and your office proposes no standards for that documentation in the Report. In other words, while there is room for the District to improve its procedures, those procedures are not out of compliance with any prior law."

Access Controls

Madison Central School District officials said: "The Report has been very helpful in identifying improvements the District can make in its procedures. However, we respectfully disagree with the Report's conclusion that Madison CSD did not "adequately" control access to its Student

Information System. The ultimate measure of the adequacy of our practices is whether there has been any unauthorized disclosure of student information. No unauthorized disclosure was documented by your audit."

OSC Response

Even though no unauthorized disclosure was identified in the results of our audit testing, this does not mean that the District adequately controlled access to its SIS. We identified several weaknesses in the District's internal controls which increase the risk for unauthorized disclosure to occur.

Unauthorized Users

Madison Central School District officials said: "With respect to Madison, the Report concludes that two staff members who entered grade changes into the system were not authorized to do so. This is inaccurate. The two individuals were a guidance counselor, who the District considers an appropriate person to access and enter grades, and an office staff member, whose assigned duties include the data entry of grades into the system as directed by teachers wishing to update student grades before report cards are printed. Similarly our review of the changes made to student demographic information concluded that all changes were made by district staff whose duties included that task."

OSC Response

The Madison CSD Teacher's Handbook indicates "once a grade is assigned to a student by a teacher, the grade may only be changed by the building principal after notification to the teacher of the reason for such change." The grade changes we identified as part of our audit testing were made by the guidance counselor and an office assistant/teacher aide, not the principal. The guidance counselor and office assistant/teacher aide are not designated as authorized users responsible for changing grades as indicated in the Handbook.

District officials told us it is the responsibility of the elementary and high school secretaries (and the guidance office staff during the summer) for changing student demographic information. Our review of change reports during our audit period found that the Treasurer made 10 changes to student demographics, even though it is not her responsibility to do so.

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

The objective of our audit was to determine whether the six districts included in our audit adequately control SIS access. To select these six districts, we classified all the districts located in the eight counties served by the Syracuse Regional Office[20] according to size (large, medium, and small), based on student enrollment. We factored in geographic locations and enrollment in order to select a sample of different sized districts from throughout the region. Our audit covered the period July 1, 2011 through April 30, 2013. We extended our scope period to perform certain tests of the districts' access controls through the following dates:

APW – November 12, 2013
Indian River – September 30, 2013
Lowville – October 7, 2013
Madison – October 1, 2013
Poland – October 7, 2013
Westhill – July 10, 2013

Our audit included the following steps relating to the audit objective:

- We interviewed district officials and staff, as well as RIC staff, and examined the districts' policies and procedures to control and monitor SIS access.

- We compared lists of active employees to lists of current SIS staff users at each district to determine if any SIS users were not district employees or if any former employees remain on the user list. We also compared lists of employees who left the districts' employment during our audit period to lists of current SIS users to verify that they were no longer active SIS users.

- We selected 229 SIS users to compare the users' job duties with user group assignments and individual user rights to determine if access rights are compatible with job duties. To choose this sample, we obtained master lists of SIS users and randomly selected 10 percent (up to a maximum of 50 in each district) of instructional and non-instructional staff users, totaling 156 users. We also judgmentally selected 73 users that we considered to have higher risk. Higher risk users included administrative users, users with add/modify permissions and users who can change closed-out grades.

- For the 90 users who had more rights than necessary to perform their job duties, we reviewed their assigned user groups for five of the districts (Indian River, Lowville, Madison, Poland and Westhill) to identify additional users who had the same incompatible rights and permissions. For APW, we reviewed a list of individual users who were granted access to various functions and compared them to the users who were designated by APW

[20] Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego and St. Lawrence

officials to perform the related function to identify those users with unnecessary access rights.

- We interviewed 115 users to determine what their job duties are and observed them navigating the SIS modules to see what access was available to them.

- We reviewed the audit logs in four districts (Indian River, Lowville, Madison and Poland) 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. Usable audit logs were not available in the other two districts (APW and Westhill).

- For districts with audit logs, we selected 70 grade changes that occurred during our audit period and determined whether these grade changes were authorized, documented and supported. The majority of our selection focused on changes made to high school students' 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

APPENDIX C

USERS, FUNCTIONS AND FEATURES BY DISTRICT

CERTAIN SIS FUNCTIONS[21]

Table 4: Grade Changes

School District	Total Number of Users Designated to Change Grades	Additional Number of Non-Designated Users With Access to Change Grades			
		RIC Staff	District Staff	SIS Vendor	Total
APW	16	51	9	0	**60**
Indian River	33	24	43	1	**68**
Lowville	24	25	13	1	**39**
Madison	18	24	13	1	**38**
Poland	23	24	6	1	**31**
Westhill	15	5	21	0	**26**
Total	**129**	**153**	**105**	**4**	**262**

Table 5: View/Modify Health Records[a]

School District	Total Number of Users Designated to View/ Modify Health Records	Additional Number of Non-Designated Users With Access to View/Modify Health Records			
		RIC Staff	District Staff	SIS Vendor	Total
APW	7	48	0	0	**48**
Indian River	30	24	4	1	**29**
Poland	19	24	0	1	**25**
Westhill	12	5	3	0	**8**
Total	**68**	**101**	**7**	**2**	**110**

[a] This function was not assessed at Madison and Lowville because these districts do not use the SIS for storing students' medical records.

[21] The RIC Staff for Indian River, Lowville, Madison and Poland is comprised of technical staff who provide SIS support at more than one of the districts. The SIS Vendor for Indian River, Lowville, Madison and Poland is the same vendor user at each of the districts.

Table 6: Change Student Demographic Information

School District	Total Number of Users Designated to Change Student Demographic Information	Additional Number of Non-Designated Users With Access to Change Student Demographic Information			
		RIC Staff	District Staff	SIS Vendor	Total
APW	14	49	5	0	**54**
Indian River	19	24	120	1	**145**
Lowville	23	25	20	1	**46**
Madison	21	24	8	1	**33**
Poland	21	24	9	1	**34**
Westhill	13	5	24	0	**29**
Total	**111**	**151**	**186**	**4**	**341**

Table 7: Add Staff User Account

School District	Total Number of Users Designated to Add Staff Users	Additional Number of Non-Designated Users With Access to Add Staff Users			
		RIC Staff	District Staff	SIS Vendor	Total
APW	11	30	15	0	**45**
Indian River	18	24	37	1	**62**
Lowville	18	25	13	1	**39**
Madison	18	24	3	1	**28**
Poland	18	24	0	1	**25**
Westhill	9	5	33	0	**38**
Total	**92**	**132**	**101**	**4**	**237**

USERS WITH UNNECESSARY ACCESS TO ASSUME-IDENTITY AND ASSUME-ACCOUNT FEATURES[22]

Table 8: Assume-Identity Feature

School District	RIC Staff	District Staff	SIS Vendor	Total
Indian River	24	64	1	**89**
Lowville	25	8	1	**34**
Madison	24	12	1	**37**
Poland	24	9	1	**34**
Total	**97**	**93**	**4**	**194**

Table 9: Assume-Account Feature

School District	RIC Staff	District Staff	SIS Vendor	Total
Indian River	24	58	1	**83**
Lowville	25	2	1	**28**
Madison	24	10	1	**35**
Poland	24	4	1	**29**
Total	**97**	**74**	**4**	**175**

[22] The SIS used by APW and Westhill do not have the "Assume-Identity/Account" features. Also, the RIC Staff shown for Indian River, Lowville, Madison and Poland is comprised of technical staff who provide SIS support at more than one of the districts. The SIS Vendor shown for Indian River, Lowville, Madison and Poland is the same vendor user at each of the districts.

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
Nathaalie N. Carey, 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 AND REGIONAL PROJECTS
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