THOMAS P. DiNAPOLI
COMPTROLLER

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

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

August 19, 2014

Casey Barduhn, Superintendent
Members of the Board of Education
Westhill Central School District
400 Walberta Road
Syracuse, NY 13219

Report Number: P3-13-9

Dear Mr. Barduhn and Members of the Board of Education:

A top priority of the Office of the State Comptroller is to help officials manage their resources efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support operations. The Comptroller oversees the fiscal affairs of local governments and 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 operations and Board governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard assets.

We conducted an audit of six school districts located in central and northern New York. The objective of our audit was to determine whether the districts adequately control access to their student information system (SIS). We included the Westhill Central School District (District) in this audit. Within the scope of this audit, we examined the District's policies and procedures and reviewed access to the SIS for the period July 1, 2011 through April 30, 2013. We extended our scope period through July 10, 2013 to perform certain tests of the District's access controls.

This report of examination letter contains our findings and recommendations specific to the District. We discussed the findings and recommendations with District officials and considered their comments, which appear in Appendix A, in preparing this report. District officials generally agreed with our findings and recommendations and indicated they planned to initiate corrective action. At the completion of our audit of the six districts, we prepared a global report that summarizes the significant issues we identified at all of the districts audited.

Summary of Findings

The District did not adequately control access to its SIS. Although the Board of Education (Board) established policies related to the confidentiality of computerized information and breach notification requirements, District officials have not established formal procedures for the administration of the SIS to ensure that access rights are assigned only to authorized users and are compatible with their roles or job duties. There is no formal authorization process to add, deactivate or modify user accounts and rights, and management does not periodically monitor user rights to ensure they are current and appropriate. In addition, management does not periodically review change reports or audit logs to identify inappropriate activity on the system. As a result, personal, private and sensitive information (PPSI)[1] in the SIS is at risk of inappropriate access and misuse.

Our audit found that 21 of the 50 user accounts tested (42 percent) included more access rights than necessary for users to fulfill their roles or job duties; these additional rights included adding new users, modifying user rights, changing student demographic information or grades and viewing and modifying health records. We also found one unidentified user, who is not a current District employee, 11 generic user accounts that were not assigned to any specific individuals, and two accounts that were each shared by two District employees, one of whom no longer works for the District. Further, District officials were not sure if change reports were available from the SIS and they were unable to provide a clearly understood audit log from the SIS. Management did not review any user changes during our audit period.

Our audit also disclosed areas where additional information technology (IT) security controls and measures should be instituted. Because of the sensitive nature of these findings, certain specific vulnerabilities are not identified in this report, but have been communicated confidentially to District officials so they could take corrective action.

Background and Methodology

The District is located in the Towns of Geddes and Onondaga in Onondaga County and operates four schools with approximately 1,850 students and 290 employees. The District's budgeted appropriations totaled $34.8 million for the 2013-14 fiscal year. These costs are funded primarily through State aid and real property taxes.

The District is governed by a five-member Board. The Board's primary function is to provide general management and control of the District's financial and educational affairs. The District has a centralized technology department (Department) headed by the Director of Technology who is responsible for directing the day-to-day Department operations and staff, which includes overseeing several software applications, including the District's SIS. The Central New York Regional Information Center (CNYRIC) houses the District's SIS, and the Western New York Regional Information Center (WNYRIC) provides technical support for the SIS to the District.

The SIS commonly contains extensive information including parent and emergency contacts, attendance, disciplinary actions, testing, schedules, grades and medical information. Therefore, the SIS includes a considerable amount of PPSI, which students and their parents entrust school districts to safeguard. In addition to providing SIS access to teachers, administrators and various

[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.

staff members, many districts also provide parents with limited access to their child's information and students with limited access to their own information.

Authorized users of the District's SIS are parents, students, teachers, administrators and various other District staff, as well as CNYRIC and WNYRIC employees involved in supporting the SIS. The District assigns access rights through 29 different user groups[2] in its SIS for 1,966 student, parent and staff users.[3] Private information in the District's SIS application includes demographic, health, course and special education information; student evaluations; student identification numbers; and current and historical grades. The student data entered into the District's SIS can also be transferred to other operating applications used throughout the District for programs such as school lunch, transportation, and special education.

Good governance and accountability require the Board and District management to establish controls to prevent unauthorized access to the PPSI and to ensure authorized users of the SIS have only approved access rights that are compatible with their role or job duties at the District. Effective controls can help to prevent the misuse or alteration of student information within the SIS and the transfer of incorrect student information to other operating applications within the District.

To achieve our audit objective, we interviewed District officials and staff and examined the District's policies and procedures to control and monitor access to its SIS. We also performed tests to determine if access was properly restricted based on the users' role or job duties and to determine if staff user accounts were assigned to active District employees.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit is included in Appendix B of this report.

Audit Results

District officials are responsible for developing IT controls to protect and prevent improper access to PPSI in the SIS. Policies and procedures should be established to ensure access is limited to only authorized users of the system and that rights assigned to authorized users are compatible with their roles or job duties. Management should periodically monitor user accounts and rights to ensure the rights agree with formal authorizations and are current and updated as necessary. Management should also periodically monitor change reports or audit logs from the SIS for any unusual activity to help ensure that only appropriate changes are being made by authorized users of the SIS.

Policies and Procedures – The Board adopted a Confidentiality of Computerized Information Policy that requires access to confidential computerized data be limited to only authorized District personnel. The Board also adopted an Information Security and Breach Notification Policy that clarifies PPSI and details how District employees would notify affected parties whose private information was, or is reasonably believed to have been, acquired without valid

[2] 27 instructional and non-instructional staff user groups, one parent group and one student group

[3] Comprising 1,660 student/parent users, 290 staff users, 11 WNYRIC employees and five CNYRIC employees

authorization. However, District officials have not established formal procedures for the administration of the SIS, such as specifying the approval levels necessary for adding users, establishing users' access rights, deactivating user accounts or periodically reviewing access rights. Without written procedures over the maintenance of user accounts, staff responsible for these functions may not understand their role, and adequate controls are not in place to appropriately restrict access to the SIS.

User Access – When access is not properly restricted, there is an increased risk that sensitive or confidential data will be exposed to unauthorized use or modification. For example, users may be able to view confidential data to which they should not have access or perform functions that they have no authority to do, such as adding a new (possibly fictitious) user, granting additional access rights for themselves or others or modifying student information, such as grades.

The District has 27 staff user groups in the SIS, each with an associated set of rights and permissions. The user groups include titles such as Clerical, Nurses, Transportation, Principal and Teachers. The Director of Technology told us all users within a user group have the same rights and permissions to either view or modify data, or both. If a staff member needs rights different than those in any established user group, the Director will create a new staff user group to grant rights specific to that user. When we reviewed reports of user rights granted to the groups and asked about the meaning of certain rights identified, the Director of Technology and WNYRIC personnel were unsure of the meaning of many of the rights and permissions within each staff user group. As a result, the Board and management do not have assurance that user rights assigned are always based on the user's role or job duties.

While the Director of Technology is responsible for assigning and modifying specific user access rights within the groups, the District Office Secretary/Board Clerk (Clerk) is responsible for adding and deactivating staff user accounts. There is no formal authorization or approval process to add or remove staff user accounts to the SIS or to assign or change user rights. The Clerk told us that she uses the Board minutes to identify personnel changes (e.g., new hires authorized by the Board) and she adds and deactivates user accounts in the SIS accordingly.[4] If a staff member leaves the District, she places the new staff user in the same group as their predecessor. However, without formal authorization from management to identify approved users of the SIS and their rights, there is no guarantee the Clerk is placing users in correct staff user groups, or identifying from the Board minutes each account that should be deactivated because of termination, retirement or change in job duties. In addition, assigning the same rights to a new user as a predecessor in the same job title does not guarantee that the user rights assigned are accurate. Lastly, management does not periodically review staff user rights after they have been assigned, further increasing the risk that user accounts and rights may not be current or appropriate.

As a result of the weaknesses identified, we compared the access rights/permissions of 50 users in 13 groups[5] to their job duties to determine whether their access is compatible and appropriate. We interviewed 18 of these users who represented each of the groups in our sample to determine

[4] The District adds CNYRIC user accounts to the SIS. However, it does not add WNYRIC user accounts to the SIS; these user accounts are added by WNYRIC.

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

what their job duties are and observed them navigating the SIS screens to see and understand what access was available to them. We found 21 of the 50 users (42 percent) tested had more rights than necessary to fulfill their job duties.[6] Further, the user groups that these users were assigned to indicated that, in fact, the number of users with permissions that are not required for their jobs is much larger. The results of our testing disclosed the following:[7]

- District guidance secretaries are responsible for changing student demographic information. However, we found 14 other users in our sample who also have the ability to change demographic information such as student age, student user identification number, address and parent contact information. The 14 users, included in seven staff user groups, are the director of curriculum, business official, Director of Technology, District office secretary, four principals, middle school secretary, high school secretary, guidance counselor, nurse, assistant principal and a WNYRIC employee. Because the Director of Technology told us user rights and permissions are the same for all users within each user group, all the other users within these seven groups are capable of making these demographic changes as well, even though it is only the guidance secretaries' responsibility to do so. In total, there are 29 users (24 staff users, three WNYRIC employees and two CNYRIC employees) in these seven user groups who are capable of making changes to student demographic information without authorization.

- The four principals told us that there are seven users[8] who are authorized to change historic grades. However, we found eight other users who can also change historic grades (the business official, Director of Technology, high school guidance counselor, a WNYRIC employee and the secretaries).[9] These eight users are included among six different staff user groups that contain a combined total of 26 users (21 staff users, three WNYRIC employees and two CNYRIC employees) who can change historic grades even though it is not within their job responsibilities to do so.

- Nurses are responsible for viewing and modifying health records; however, we found that four other users (the Director of Technology, a WNYRIC employee and two principals) could view and modify health records. These four users are in a group that contains a combined total of eight users (three staff users, three WNYRIC employees and two CNYRIC employees) who can view and modify health records without authorization.

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

[7] WNYRIC officials told us WNYRIC SIS support staff require full access rights to the SIS in order to assist the District with troubleshooting on a day-to-day basis. We did not include SIS support staff as exceptions in our testing. However, we did include other WNYRIC and CNYRIC technical staff (e.g., programmers and technicians) in our exceptions because they were granted full access rights to the SIS and they only need occasional access for troubleshooting. Rather than provide full access rights to these users all the time, the District should grant them the necessary access only when they need it.

[8] High school principal, middle school principal, two elementary school principals, high school assistant principal, middle school assistant principal and the middle school guidance secretary

[9] High school secretary, middle school secretary, District office secretary and high school guidance secretary

- Only the District office secretary is responsible for adding and deactivating staff user accounts in the staff user groups. We found 16 additional users (director of curriculum, business official, Director of Technology, four principals, director of transportation, two guidance secretaries, middle school secretary, high school secretary, typist, nurse, assistant principal and a WNYRIC employee) who also can add, modify or deactivate staff user accounts. These 16 users are included among eight user groups that contain a combined total of 38 users[10] (33 staff users, three WNYRIC employees and two CNYRIC employees) who can add or deactivate staff user accounts even though it is not within their job responsibilities to do so. In addition, these 38 users also have the ability to modify the specific rights and permissions within the user groups, even though the Director of Technology is the only individual responsible for modifying rights and permissions.

- Only the guidance secretaries are responsible for adding and modifying student/parent accounts, but we found 16 other users (director of curriculum, business official, Director of Technology, District office secretary, four principals, dispatcher, director of transportation, middle school secretary, high school secretary, guidance counselor, nurse, assistant principal and a WNYRIC employee) also have permission to add and modify the student/parent accounts. The 16 users are in 10 user groups that contain a combined total of 31 users (26 staff users, three WNYRIC employees and two CNYRIC employees) who can add and modify student/parent accounts even though their responsibilities may not require them.

The Director of Technology was not aware that these users had more permissions than necessary. The majority of these users are District staff, but also include WNYRIC and CNYRIC technical staff (e.g., programmers and technicians) who rarely access the SIS to assist the District with troubleshooting and, therefore, do not need all the user rights they have been granted in the SIS. It is important for the District, in conjunction with WNYRIC, to review and update user permissions in order to help reduce the risk that sensitive or confidential student information could be compromised.

We also compared a list of all the District's active employees to a list of the 290 current staff users of the SIS to determine if any users of the SIS are not District employees or if any former employees remain on the current user list. One user account with teacher access rights was not on the District's list of active employees. After bringing this to the attention of the Director of Technology, he told us he was not familiar with the name of the staff account and he deactivated it. In addition, we also found 11 user accounts with generic user names. The Director of Technology told us the accounts were created as sample or test accounts. While these accounts have limited access to the SIS, District officials should deactivate them if they are no longer needed, to prevent unauthorized use. Lastly, we found two accounts were shared by four people (two people sharing one account each), one of whom is no longer employed by the District. In addition, the other three users have their own unique user accounts. The sharing of user accounts increases the risk of unauthorized access to SIS data.

[10] One user (of the 38) is the former district office secretary. Even though she is no longer responsible for adding, modifying and deactivating staff users, she continues to have this capability because she was not removed from the 'DO secretary' user group when she became the high school secretary.

Report Monitoring – Audit logs or change reports maintain a record of activity or show changes or deletions made in a computer application (e.g., grade changes or adjustments to user account access).[11] 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. Because we found that user access was not always assigned according to job duties, it is even more important that District officials monitor user activities to ensure appropriate use.

District officials do not monitor user activity in the SIS and were not aware of any change reports available to review changes made by users. At our request, they provided an audit log report; however, the report is complex and difficult to use and does not clearly show what user actions were taken. In addition, the Director of Technology was not able to explain what the specific audit log report fields meant in terms of changes made since it was his first time running the report. Because the District was not sure if change reports are available and the audit log did not provide clear information on changes made, District officials would not be able to determine whether there had been any unauthorized user activity by the 21 users in our audit sample who had more capabilities in the SIS than their job duties required, or by the 14 current user accounts that were not for active employees or were shared accounts. Furthermore, it is the District's practice to delete all user activity around the end of each school year; therefore, even if the audit logs were clear, they would not have shown user activity prior to July 30, 2013. When audit logs or change reports are not generated and reviewed, management cannot be assured that unauthorized activities are detected and adequately addressed.

Recommendations

1. District officials should establish procedures for the administration of the SIS, including a formal authorization process to add, deactivate or change user accounts and rights. Officials should periodically monitor user access rights to ensure they are as authorized.

2. District officials should evaluate the user permissions currently assigned to each user group and update the permissions or groups as needed to help ensure that individual users' access rights are aligned with their roles or job duties.

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

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

5. District officials should work with their SIS provider to gain an understanding of the audit log reports and determine if the audit log report format can be modified, or change reports produced, to be more useful. If useful reports can be generated to monitor activities, District officials should periodically review the reports for unusual and inappropriate activity.

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

6. District officials should evaluate the feasibility and usefulness of retaining SIS user activity logs beyond the current fiscal year.

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of the General Municipal Law, Section 2116-a (3)(c) of the Education Law, and Section 170.12 of the Regulations of the Commissioner of Education, a written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and forwarded to our office within 90 days. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. The Board should make the CAP available for public review in the District Clerk's office.

We thank the officials and staff of the District for the courtesies and cooperation extended to our auditors during this audit.

Sincerely,

Gabriel F. Deyo

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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

WESTHILL CENTRAL SCHOOL DISTRICT

SARAH E. VANLIEW
Executive Director of
Curriculum/Instruction
Phone (315) 426-3215

CASEY W. BARDUHN
Superintendent of Schools
400 Walberta Road
Syracuse, New York 13219-2214
Phone (315) 426-3218
Fax (315) 488-6411

STEVEN E. SMITH
Assistant Superintendent for
Business Administration
Phone (315) 426-3210

November 21, 2013

Ms. Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
Division of Local Government &
School Accountability
State Office Building, Room 409
333 East Washington Street
Syracuse, NY 13202-1428

RE: NYS OSC Report No. P3-13-9, Access to Student Information Systems

Dear Ms. Wilcox:

I acknowledge receipt of the NYS Comptroller's audit. The required corrective action plan will be forwarded under separate cover. Following are my thoughts on the audit.

The first paragraph of the NYS Comptroller's management letter says:

> *A top priority of the Office of the State Comptroller is to help officials manage their resources efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support operations. The Comptroller oversees the fiscal affairs of local governments and 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 operations and Board governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard assets.*

This audit did not identify any strategies to reduce costs, identify strategies to safeguard assets, or improve efficiencies. With respect to this audit and the potential risk for unauthorized access and altering of data in student information systems, I certainly would not characterize Westhill as a high risk for this type of behavior. Ninety nine percent (99%) of our teachers were rated effective or highly effective and Cherry Road Elementary School was recently named a 2013 National Blue Ribbon School.

"Westhill . . . Where Educational Excellence is a Tradition"

As performance based measures are implemented through New York's education reform agenda, I understand the comptroller's desire to strengthen internal controls statewide for ensuring the accuracy of student grades. Because Westhill Central School District was the pilot school district for the comptroller's review of its student information systems, we will take the initiative to review our policies and procedures for safeguarding the integrity of student grades and protecting student information. The district will work collaboratively with the regional information centers with which this service is contracted.

Sincerely,

Casey W. Barduhn
Superintendent of Schools

CWB:psr

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

We reviewed access to the District's SIS for the period July 1, 2011 through April 30, 2013. We extended our scope period through July 10, 2013 to perform certain tests of the District's access controls.

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

- We interviewed District officials and staff, as well as WNYRIC and CNYRIC staff, to gain an understanding of the District's SIS application and authorized users, assignment and monitoring of user access rights to the SIS, and IT policies and procedures.

- We compared a list of current active employees to a list of current SIS staff users to determine if any users of the SIS are not District employees or if any former employees remain on the current user list. We obtained the most recent employee user list from the SIS and obtained an employee master list from the Payroll Department. We also compared a list of employees who left District employment during our audit period to the list of current SIS users to verify they were no longer active SIS users.

- We selected 50 users of the SIS to compare the users' job duties with user group assignment and individual user rights to determine if access rights are compatible with job duties. We obtained a master list of SIS users and randomly selected 10 percent of instructional and non-instructional staff users for a total of 31 users and judgmentally selected 19 users that we considered to have higher risk. Higher risk users included users who are not on the list of current active employees, but are on the list of SIS users, administrative users, users with add/modify permissions, users who can change historical grades and users who have access to change a student or parent user name or password.

- We interviewed 18 users to determine what their job duties are and observed them navigating the SIS screens to see and understand what access was available to them.

- We also selected 17 parent/student users to verify the users only have view-only rights as a group and as individuals. We obtained the parent/student user list and randomly selected 1 percent of parent/student users.

We conducted this performance audit in accordance with GAGAS. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.