



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

September 2015

Mr. Michael Piccirillo
Superintendent of Schools
Saratoga Springs City School District
3 Blue Streak Boulevard
Saratoga Springs, New York 12866

Report Number: S9-15-44

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

A top priority of the Office of the State Comptroller is to help school district officials manage their resources efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support district operations. The Comptroller oversees the fiscal affairs of districts statewide, as well as compliance with relevant statutes and observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving district operations and Board of Education governance. Audits also can identify strategies to reduce district costs and to strengthen controls intended to safeguard district assets.

We conducted an audit of six school districts across New York State. The objective of our audit was to determine whether the districts adequately control access to student grading information systems. We included the Saratoga Springs City 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 grade book systems for the period July 1, 2013 through November 30, 2014. 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 draft report of examination letter contains our findings and recommendations specific to the District. Our audit also examined the adequacy of certain information technology (IT) controls. Because of the sensitivity of some of this information, we did not discuss the results in this letter but instead communicated them confidentially to District officials. We discussed the findings and recommendations with District officials and considered their comments, which appear in Appendix A, in preparing this report. District officials indicated they plan to initiate corrective action. Appendix B contains our comments on issues raised in the District's response. At the

completion of our audit of the six districts, we prepared a global report summarizing the significant issues we identified at all the districts audited.

Summary of Findings

We found the District does not adequately control access to the Student Grade System (System). District officials did not appropriately use the System's lock out function to help restrict grade changes. In addition, the District does not have policy guidance detailing the process or written documentation requirements for when an official must make a grade change and how it should take place. Consequently, District officials make grade changes with little or no oversight. We found that grade changes made by non-teachers after the marking periods had closed lacked documentation to support the changes 61 percent of the time. In addition, we found non-teachers routinely increased student grades from a failing 64 to a passing 65 without policy authorization. These grade changes have resulted in grades being under-reported to the State Education Department.

We also found the District has not adopted written policies and procedures for adding users, establishing users' access rights, deactivating or modifying user accounts; granting user permissions and monitoring user access to the System. District officials do not periodically review users' access rights for appropriateness, review audit logs, and monitor employees' use of System override features that allow them to assume the access rights of other users.

These weaknesses jeopardize the integrity of the students' grades and increase the risk that staff with appropriate System permission can inappropriately modify student grades.

Background and Methodology

The District is located in the City of Saratoga Springs and in portions of the Towns of Greenfield, Malta, Milton, Saratoga and Wilton in Saratoga County. The District operates eight schools (six elementary, one middle and one high school) with approximately 6,400 students and 1,000 employees. The District's budgeted appropriations totaled \$112.6 million for the 2013-14 fiscal year. These costs are funded primarily through State aid and real property taxes.

The District is governed by a nine-member Board of Education (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 Assistant Superintendent of Technology 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 Grading System (System). The System is housed onsite at the District. The North East Regional Information Center (NERIC) provides technical support for the System at the District.

The System is an electronic grade book system that maintains student class rosters in which teachers input student grades and track academic progress. This System is a database that tracks students' grades (input by District staff) and is used to monitor student performance, generate student report cards and maintain student permanent records (i.e., transcripts). Although teachers

may maintain an alternate grade book system, all grades must be entered into the System, which serves as the official District record. Generally, teachers enter/edit grades throughout the marking period and submit final grades by an established date every marking period. Grade changes that occur after the submission of final grades need to be done by a System user that has extended permissions that allow them to make changes after the close of the marking periods.

Students and their parents entrust the District to preserve the confidentiality and integrity of this information. Authorized users of the District's System include parents, teachers, administrators and various other District staff, as well as NERIC employees and the vendor, who are involved in supporting the System. The District assigns access permissions for the 9,100 users¹ in its System through 19 different user groups.²

To accomplish our audit objective, we interviewed District officials and employees. We also examined District policies and procedures to control and monitor access to the System. We performed tests to determine if student grade modifications were appropriately authorized and supported by documentation. We tested audit logs and reviewed user activity to determine if student grade modifications adhered to District policies and procedures and whether changes were compatible with users' roles and job duties. We also determined whether staff user accounts were assigned to active District employees.

Audit Results

District officials are responsible for developing and monitoring System controls to preserve data and prevent unauthorized access or modification to the System. The Board and management should establish policies and procedures to ensure access is limited to authorized System users and that users' permissions are compatible with their roles or job duties. District officials should periodically review user accounts and permissions to ensure the permissions agree with formal authorizations and are current and updated as necessary. Only authorized District staff should enter or modify student grades, and all grades should be supported by adequate documentation. In addition, District officials should periodically monitor change reports or audit logs from the System for any unusual activity to help ensure that only authorized System users are making appropriate changes. Effective physical and IT controls help preserve the System's confidentiality and integrity.

The District does not adequately control access to the System, which has resulted in grade changes with no supporting documentation. The District does not appropriately use the System's lock out function to restrict grade changes. Specifically, we found that grade changes made by non-teachers after the marking periods had closed lacked documentation to support the changes 61 percent of the time. In addition, the District does not have policy guidance that details the process or written documentation requirements for when a grade change must take place. Further, the District has

¹ The District has 19 different active user groups, some of which include administrators, census, counseling, faculty, parents, teachers, students and super-users. A super-user is essentially a system administrator and has unlimited access permissions.

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

other IT weaknesses that put the System at risk of inappropriate use or manipulation, and ultimately places the District at risk of unauthorized grade changes.

Lock Out Dates

The District's System allows teachers to enter and modify their own students' grades during each marking period until a pre-determined lock out date. The lock out date is a date in the marking period when grades are to become final and entered into the System. The District's Program Coordinator sets these dates before the start of each school year based on student report card reporting dates. After a lock out date, teachers can no longer enter or modify student grades. Only staff with heightened System permissions may make necessary changes then.³ These heightened permissions are System permissions that enable authorized officials to modify student grades until a final year-end marking period lock out date. Management provided these permissions to 175 District officials, including guidance counselors, guidance clerks, elementary and middle school principals, assistant and vice principals, teachers, a school psychologist, a gym teacher, a library media specialist, an office clerk, a medical clerk, a typist and IT department staff. The proper use of lock out date controls help prevent grade modifications without authorization after the close of a marking period.

We found the District does not appropriately use the lock out function to restrict grade modifications. Specifically, we found the Program Coordinator and four additional technology staff members modified the established lock out date 34 times during the 2013-14 school year, without a principal's written approval or authorization. This allowed teachers to edit grades after the District-established deadline. During the audit period, there were 75,632 grade modifications made by teachers; 11,918 modifications (16 percent) took place after the initially established lock out date. For example,

- The lock out date for the first marking period in the 2013-14 school year was changed nine times, extending the original November 12, 2013 date out as far as one year.
- The lock out dates for the second and third marking periods in 2013-14, originally established at February 5, 2014 and April 25, 2014, respectively, were changed 19 times. Therefore, grade modifications extended out as late as the end of the school year (June 27, 2014).
- Lastly, the final marking period was changed six times, which extended the marking period from June 20 to July 1, 2014.

District technology staff indicated that the need to input grades after the lock out date occurs on a regular basis. Current lock out date controls require users with heightened permissions to make the changes. The Program Coordinator told us that bypassing the lock out date was more productive than taking the time to obtain the appropriate permissions to modify the grades. Due to a lack of management oversight and inconsistency in following established procedures, grade modifications occurred well beyond District-established timeline controls. By allowing staff to

³ Generally, teachers do not have access to this level of user permissions.

circumvent established controls, the risk that unauthorized grade modifications could occur and go undetected is greatly increased.

Grade Modifications

The official record of student grades should be accurate and preserved to ensure its integrity. The System serves as the historical record of student performance, credit accumulation, report cards and student transcripts that are relied upon by students and parents to assess student standing. In addition, educators and the public evaluate school districts locally, regionally and nationally based on common student performance measures. Other schools, colleges and potential employers use student grades and transcripts to determine student aptitude. District policies should include documentation requirements to support changes to students' grades, especially when done by someone other than the students' teacher (generally after the close of the marking period).

We found the District does not adequately control grade changes. The District does not have policy guidance that details the process or written documentation requirements for when a grade change must take place. From our testing, we found that grade changes made by non-teachers after the marking periods had closed lacked supporting documentation 61 percent of the time. These modifications generally included changing grades from failing to passing and increasing grades (e.g., original grade was changed from a 70 to an 85) without any supporting documentation from the teacher.

Heightened Permission Changes – As noted previously, teachers enter grades throughout the marking period and submit final grades by an established date every marking period. A System user with heightened permissions⁴ must make grade changes after the close of a marking period. During our audit period, high school teachers and heightened permission users made 77,827 grade changes. The user group with heightened permissions made 2,195 of these changes. We tested 90 grade changes⁵ made by this user group (typically guidance counselors) and found that 55 (61 percent) could not be supported with written documentation from the teacher, or other appropriate individual, authorizing the change. When reviewing the unsupported changes, we found 36 (66 percent) changed a grade from failing to passing, 16 (29 percent) increased or decreased a grade, and three changes (6 percent) changed a grade from no grade to 65 or better.

Some examples of unsupported grade changes that District officials with heightened permissions made included:

- In July 2013, an Earth Science grade was changed from a 54 to 65 for the 2012-13 school year. The counselor indicated a teacher had called and requested the change.
- In June 2014, an Algebra 1 with lab grade was changed from a 52 to 65 for the 2013-14 school year. The counselor indicated the teacher verbally communicated that the student grade should be changed because of extra effort towards the end of the year.

⁴ For testing purposes, we did not test grade changes made by teachers during the marking period.

⁵ See Appendix C, Audit Methodology and Standards, for details on our sample selection.

- In June 2014, a guidance department secretary changed a Chemistry Regents grade from none to 54 for the 2013-14 school year because she indicated she was the only one in the office available when the teacher requested the change.

Changing Grades From 64 to 65 – We found District guidance counselors routinely increased grades from a failing 64 to a passing 65. Specifically, we found these users with heightened permissions made 14 grade changes from a 64 to a 65 during our audit period. Twelve of these changes had no written documentation from a teacher to support the change. The Head Guidance Counselor at the high school indicated that District policy requires that final grades of 64 be rounded to 65. The Head Guidance Counselor and other colleagues indicated that, at the end of the school year, they review final grades submitted to ensure there are no obvious errors and will, at this time, change grades from a 64 to a 65. For example, in July 2014 an Applied English 12/BOCES grade was changed from a 64 to a 65 for the 2013-14 school year. The counselor indicated that the most likely reason for the change was that a teacher asked him to make the change. However, there was no documentation to support this change.

The High School Principal acknowledged that there is no District-wide policy to change grades from a 64 to a 65. However, he told us that it was a past practice to round grades from 62.5 (failing) to a 65 (passing). The Principal stated that counselors should contact teachers who have issued final grades of 64 to determine whether they want the grade changed to a 65. Further, the Principal told us that some counselors may have changed grades with the understanding that this is a District policy.

We reviewed the grades submitted to New York State Department of Education (NYSED) for the required annual filing at year-end. We found the District had reported one grade of 64 but reported over 300 grades of 65.

Because of the District’s lack of policy guidance, counselor-level staff are changing grades from failing to passing without any documentation and authorization from the teacher. This increases the risk that student grades and transcripts are not accurate.

Prior-Year Grade Changes – We reviewed the System log of grade changes made by users with heightened permissions. We found they made 126 student grade changes between June 2013 and November 2014 that pertained to previous school years as far back as 2009-10. We judgmentally selected and tested 22 prior-year grade changes and found three were related to the 2010-11 school year, 10 related to the 2011-12 school year, and nine related to the 2012-13 school year. For example:

- In August 2013, a grade for an English course taken in the 2012-13 school year was changed from a 69 to a 78 without any documentation as to the basis or necessity of the modification.
- In October 2014, 15 months after the close of the applicable school year, a grade in a technology elective course taken in the 2012-13 school year was changed from a 67 to an 85 without any documentation as to the basis or necessity of the modification.

Further, guidance counselor-level officials were unable to provide an explanation for a total of 21 of these prior-year grade changes.

Guidance counselor-level officials explained that these changes occur as the result of teachers specifically asking them to make the changes; however, these authorizations are often verbal and are not documented. The failure to document approvals and the reasons for necessary student grade modifications increases the risk that such changes are not properly authorized and supported, which places the integrity of the student's permanent record at risk. For example, we reviewed the final grade report sent to SED for the 2013-14 school year, which contained 19,101 grades. We found 59 separate instances where the grades submitted to SED were lower than the permanent grade record maintained by the District. Grades on the SED report ranged between one and 42 points lower than those maintained by the District.

Information Technology

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

Policies and Procedures – The Board adopted an Information Security Policy Manual. The policy manual contains a variety of documents including policies on acceptable use, information classification, information handling, password management, security incident management and data breach protection.

The District has not adopted written policies and procedures for adding users, establishing users' access rights, deactivating or modifying user accounts, granting user permissions and monitoring user access. The District has a process in place for adding new users, which includes the personnel department assigning a user group to new employees based on the job for which the employees have been hired. The IT Department will assign the employee to that user group in the System and grant the employee the system permissions associated with that group. If the permissions granted prove to be inadequate for the employee to perform all the duties of a particular job, or if IT personnel is unfamiliar with the duties associated with a particular job, they will confer with the head of the department in which the employee works and adjust permissions granted accordingly. However, District officials do not periodically review users' access rights for appropriateness, and do not review audit logs (System-generated trails of user activity) for potentially unauthorized activity. Finally, District officials do not monitor employees' use of powerful System features that allow them to assume the access rights of other users.

Without written procedures over the maintenance of user accounts, staff responsible for these functions may not understand their role, and there is an increased risk that access to the System will not be properly restricted.

User Access – The Program Coordinator is responsible for adding and deactivating staff user accounts in the System; however, anyone with the super-user permissions (32 users) can add and deactivate staff user accounts. Further, we found 175 users⁶ with the ability to modify student grades at any point during the school year. These users include District IT staff, administrators, counselors, principals and various other staff (this group generally does not include teachers). However, we found that only 21 of these users actually made grade modifications. IT staff attribute the large number of users that have not made grade changes to general user groups that include a bundle of heightened permissions. By granting so many users the ability to change grades, the District increases the risk of unauthorized grade changes being made. For example, an IT staff person made 183 student grade changes but could not provide any written documentation supporting the basis for the changes. This user indicated she assisted staff that were not as familiar with the System.

We also found that the System contains active user accounts for 27 former District employees. District officials told us that these former employees' accounts remained active due to a lack of awareness and monitoring. District IT staff are not notified of an employee's retirement or other separation from the District and the need to deactivate the applicable account.

By not properly restricting user privileges and accounts, the District is putting its System's integrity at risk and there is an increased risk that sensitive or confidential data will be exposed to unauthorized use or modification. For example, users may be able to view confidential data to which they should not have access or perform functions that they have no authority to do, such as adding a new user account or modifying student information (e.g., grades and demographics). This increases the possibility of unauthorized grade modifications and lack of accountability over the System.

Assume-Identity/Assume-Account Features – District officials should strictly control the ability to grant or modify user rights in the System. Individual users should not have the capability to assign themselves additional user rights beyond those rights they have already been authorized. However, the District's System allows certain users to assume the identity or the account of another user.

- The assume-identity feature allows a user to retain their own rights/permissions while accessing student information for students assigned to the user whose identity they assume. During our testing, we identified 185 users⁷ in six user groups with the ability to assume identities of another user. In total, these six user groups (containing 170 staff users, 10 NERIC employees and five System vendor employees) can perform this assume-identity function.
- The assume-account feature is similar to the assume-identity feature in that the user retains their own rights/permissions. However, it allows a user to assume the account of another user and inherit all the given rights/permissions of that user. We identified 37 users who have the ability to assume the account of another user. These 37 users are in three user

⁶ Some users within these groups are assigned to more than one group.

⁷ Ibid.

groups (containing 22 staff users, 10 NERIC employees and five System vendor employees) who can perform this powerful function.

Audit Logs – Audit logs 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.

We found the District does not monitor audit logs or change reports. Despite having the ability to produce audit logs, the District did not generate audit logs or review them for potentially unauthorized changes.

District officials indicated that they would review audit logs only if an issue was brought to their attention. 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. Restrict the ability to make grade changes after the close of a marking period to designated individuals and ensure that documentation is retained to show who authorized the grade change and the reason for the change.
2. Adopt policy guidance regarding the utilization of the lock out function and what procedures must be followed to bypass this control.
3. Periodically review the bypassing of the lock out function and determine the appropriateness of the changes.
4. Adopt policy guidance relating to the procedures and requirements for making grade changes in the current year and for prior years.
5. Periodically review the grade changes made by the heightened permission users and determine the appropriateness of the grade changes.
6. Update the annual reporting to the State Education Department to ensure accurate grade records are being reported.
7. Review current procedures for assigning user access rights and strengthen controls to ensure that individuals are assigned only those access rights needed to perform their job duties. District officials should monitor user access rights periodically.

8. Evaluate the user permissions currently assigned to each user group, develop a process to verify that individual users' access needs are compatible with the rights of the assigned groups, and update the permissions or groups as needed.
9. Review current user permissions and deactivate inactive users from the System.
10. Consider whether the assume-identity and assume-account features are appropriate for use.
11. Periodically review available audit logs for unusual or inappropriate activity.

The Board should:

12. Adopt written policies and procedures for adding users, establishing users' access rights, deactivating or modifying user accounts, and monitoring user access.

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of the New York State General Municipal Law, Section 2116-a (3)(c) of the 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 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 Saratoga Springs City School District for the courtesies and cooperation extended to our auditors during this audit.

Sincerely,

Gabriel F. Deyo
Deputy Comptroller

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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

SARATOGA SPRINGS CITY SCHOOL DISTRICT
MACFADDEN ADMINISTRATION BUILDING
3 BLUE STREAK BLVD., SUITE 204
SARATOGA SPRINGS, NEW YORK 12866-1232

MICHAEL M. PICCIRILLO
Superintendent of Schools

Telephone: (518) 583-4708
Fax: (518) 584-6624
E-mail: m_piccirillo@saratogaschools.org

June 8, 2015

Ann C. Singer, Chief Examiner
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417

Dear Ms. Singer:

I am writing in response to the May 21, 2015 exit discussion regarding the preliminary draft findings of the Office of the State Comptroller's Access to Student Grading Systems examination. I want to thank you for the thorough review of the draft findings and the opportunity to respond to the information presented.

The Saratoga Springs City School District recognizes the value of audits as a means to identify opportunities for improving district operations through policy and practice. As such, we take the findings of an audit seriously and compliance with the recommendations for improvement as a leadership responsibility. Therefore, in this letter you will find responses to each of the recommendations made in the draft findings as action statements for improvement.

Additionally, public schools operate in an increasingly politicized environment. Thus, recommendations for improvement must be seen as just that. This requires conclusions to thoughtfully and accurately use language, therefore, avoiding intentional or unintentional magnification of a concern. Furthermore, supporting data must be used to appropriately support a contention. For these reasons, you will find in this letter responses to particular sentences, phrases and individual words, which we believe do not accurately portray the circumstances and we kindly ask you to consider revising or deleting them.

Responses to aspects of the letter we take umbrage with will be addressed by section. The 12 recommendations will be addressed individually at the end of the response letter.

Summary of Findings

- (p. 2) *District officials did not appropriately use the Systems' lock out function to help restrict grade changes.*
 - The use of the descriptor “District officials” is misleading and connotes members of the District Cabinet i.e., superintendent of schools, assistant superintendents, directors etc. use the lock out function. Though these individuals may have permissions to use the lock out function, there is no indication in your findings that in fact any of these employees have used the function. The lock out function is used at the building level by the Program Coordinator II at the request of the Guidance Department Head. Therefore, the descriptor should specifically identify which titled employees actually use the lock out function. By doing so, the misperception of associating “District official” with members of the Administrative Cabinet can be avoided.
 - Second, the contention that the lock out function was not used appropriately is a generalization based on a finding regarding the opening of grades beyond lock out dates. The presumption is two-fold: when grades are opened they are opened permanently; there are no legitimate reasons to open grades after a lock out date has passed. In reality, when grades are opened beyond the lock out date, thus, bypassing the lock out function, they are opened temporarily by the Program Coordinator II to allow for a legitimate change by a guidance counselor at the request of a teacher. The lock out resumes immediately following the grade change, hence, the grades are not open for any length of time beyond completing the quick function of making a grade change as implied later in the report. Furthermore, in our opinion there are many legitimate mitigating circumstances, which require the opening of grades beyond the lock out date such as a student who was out of school for medical reasons, transfer students whose grades from a previously attended school do not follow in a timely manner and other unforeseen and uncontrollable circumstances. In addition, a contention is made later in the report that student grades are not reported accurately to the State Education Department, because the changes take place after the date for uploading quarterly grades. Grades can be changed in the State database up until the final upload in July. There was one instance when grades were changed beyond this date. We have no control over the dates set for uploading grade data to the state. However, we do have control over accurately recording a student’s progress to inform decisions about appropriate programming. Unfortunately, the lives of our students do not always conform perfectly to the dates for grade reporting set by NYSED, nor do they always conform to internal guidelines such as lock out dates. We request clarification, modification or removal of this finding as written.
- (p. 2) *District officials make grade changes with little or no oversight.*
 - We reiterate as in the previous item the use of the descriptor “District officials” is not accurate and should be replaced with specific job titles. Therefore, it stands to reason that District officials and building administrators in fact made no grade

See
Note 1
Page 23

See
Note 2
Page 23

See
Note 3
Page 23

changes. All changes were made by guidance counselors at the request of teachers. The statement of little or no oversight is also misleading. Grades are changed by guidance counselors at the request of teachers throughout the year for some of the reasons previously stated. Prior to closing their grade records for the year, teachers completed grade verification sheets as a means of cross checking grade accuracy. To imply there is little or no oversight is erroneous. Again, we ask for specific identification of positions being referenced and not the use of broad terminology such as the word district.

- (p.2) *In addition, we found non-teachers routinely increased student grades from failing 64 to a passing 65 without policy authorization.*
 - We again ask for a more accurate and specific identification in reference to the descriptor “non-teachers”, so as not to imply administrators, non-instructional personnel or even parents made grade changes. Guidance counselors make grade changes at the request of teachers. See
Note 4
Page 23
 - Your own data does not support the use of the term “routinely” in describing grade changes from 64 to 65. On page 5 of the draft report it is stated that 77,827 grade changes were made and later in the report on p. 7 it is noted that over 300 grades of 65 were reported. In other words, grade changes to 65 occurred less than 1% of the time in relation to total grade changes, establishing that this is not a routine action. In addition, the specific 300 grades changed to a 65 occurred as a result of a long standing practice dating back to the 1970’s. We acknowledge the need to change the practice and have taken action to do so, but this practice should not be construed as routine in the sense that it happens on a regular day to day basis. It is routine only in that it had occurred annually as a result of a long standing practice. We ask for a change in the language used in this part of the report, specifically the term “routinely”. See
Note 4
Page 23
- (p. 2) *These grade changes have resulted in inaccurate reporting to the New York State Education Department.*
 - As stated previously, the State Education Department establishes dates for the uploading and reporting of quarterly grade data. However, historical data can be changed on student transcripts to accurately reflect a students’ grade. In the real world of grade reporting at the local level student’s lives do not always conform to these rigid deadlines. Consequently, unforeseen long term medical absences, mental health issues, incarceration and other circumstances require schools to be more flexible in the time frames they impose on grading in certain circumstances, which will not always meet the timelines established by the state. We request clarification, modification or removal of this finding as written. See
Note 5
Page 23
- (p. 2) *The weaknesses significantly jeopardize the integrity of the students’ grades and increase the risk that staff with appropriate System permission can modify student grades as they see fit.*
 - This statement of finding implies grade changes are made arbitrarily and capriciously by any staff with Systems permissions. Again, data on page five of the report refutes the finding. According to the report, during the audit period See
Note 6
Page 24

77,827 grade changes were made with 2,195 changes made by the user group with heightened permission. The percent of grade changes made by the user group with heightened permissions is 2.8%, a small percent of the total. Additionally, the phrase, “can modify student grades as they see fit” is subjective and implies the potential for a lack of professionalism on the part of these users. We reiterate, all grade changes are made by school counselors at the request of teachers and these changes are verified by teachers at the end of the school year when teachers sign a grade verification form. Admittedly, there are no written policies as of yet governing grade changes and a system for recording grade changes with cause and approval needs to be put in place. We request modification or removal of this finding as written.

Audit Results

- (p. 3) *The District does not appropriately use the System lockout function to restrain grade changes.*
 - We would ask for clarification on the term “appropriately” as used in this statement. Again, the District acknowledges the need for written documentation supporting grade changes. However, the grade changes made as stated previously are the result of the natural course of event in students’ lives, which do not fit neatly into the timeframes for grade reporting established. The System lock out function restricts users from making changes after lockout dates have passed except in those instances where student grades should be changed to accurately reflect their academic standing. Grades are unlocked temporarily by the Program Coordinator II at the request of a counselor to make a change and immediately re-locked. To not allow for any grade changes after the lock out date would result in student grades being inaccurate and could impact their transcripts. We ask for modification or removal of this finding as written.

See Note 2 Page 23

Lock Out Dates

- (p. 4) *Management provided these permissions to 69 District officials, including guidance counselors, guidance clerks, elementary and middle school principals, assistant and vice principals, teachers, a school psychologist, a gym teacher, a library media specialist, an office clerk, a medical clerk, a typist and information technology staff.*
 - There are 13 total employees who use there permissions to make grade changes. Guidance counselors comprise 12 of the 13 users and one is a building assigned Instructional Technologist. The Instructional Technologist will assist teachers in making grade changes at their request as a result of their lack of confidence with navigating the student management system. Counselors, as stated previously, make grade changes only at the request of a teacher. We ask for modification or removal of this finding as written.

See Note 7 Page 24

- (p. 4) *We found the District does not appropriately use the lockout function to restrict grade modification.*
 - The only persons who would be able to request that the lockout date be changed (for teacher requested grade modifications) would be the High School and Middle School Guidance Department Heads. The only person who makes the change to this lock out date 99% of the time is the Program Coordinator II. Other Super Users have this ability and only use it in the event that the Program Coordinator II is not available for the request from these Department Heads. We ask for modification or removal of this finding as written

See
Note 2
Page 23

Grade Modifications

- (p.5) *We found the District does not adequately control grade changes.*
 - Again, only guidance counselors and the Instructional Technologist make grade changes and these occur only at the request of a teacher. We ask for modification or removal of this finding as written.

See
Note 8
Page 24

Information Technology

- (p.7) *The District has not adopted written policies and procedures for adding users, establishing users' access rights, deactivating or modifying user accounts, granting user permissions and monitoring user access.*

See
Note 9
Page 24

Policy and Procedure Section

The district has created a policy and procedure manual for the creation and maintenance of accounts. Our SSCSD IT Security Policy Manual (pages 20-22) is referenced below:

PURPOSE

This policy defines the control requirements for the secure management of accounts on Springs City School District (District) computer and communications systems.

SCOPE

This policy applies to all District computer systems and facilities, with a target audience of District Information Technology employees and partners.

POLICY

Authorization

Access Control Authorization Forms - Requests for the addition, deletion, and modification of all user IDs, credentials, and other identifier objects on District computer and communications

systems must be submitted on a form authorized by the worker's immediate supervisor or manager.

Granting Information System Privileges - Computer and communication system privileges must be granted only by a clear chain of authority delegation.

Granting Access To Organization Information - Access to District information must always be authorized by a designated Owner of such information, and must be limited on a need-to-know basis to a reasonably restricted number of people.

Awareness and Training

User Agreement To Abide By Security Requirements - Before they are granted access to District information systems, all users must provide documented evidence of their agreement to comply with District information security and privacy requirements. The ways that this evidence can manifest are defined exclusively by the Information Technology Department.

Account Definition

Unique User ID And Password Required - Every user must have a single unique user ID and a personal secret password for access to District multi-user computers and computer networks.

Non-Anonymous User IDs - All user IDs on District computers and networks must be constructed according to the District user ID construction standard, must clearly indicate the responsible individual's name, and under no circumstances are such user IDs permitted to be generic, descriptive of an organizational title or role, descriptive of a project, or anonymous.

Unique User IDs - Each computer and communication system user ID must uniquely identify only one user. Shared or group user IDs must not be created or used.

Generic User IDs - User IDs must uniquely identify specific individuals and generic user IDs based on job function must not be created or used.

Re-Use Of User IDs - Each District computer and communication system user ID must be unique, connected solely with the user to whom it was assigned, and must not be reassigned after a worker or customer terminates their relationship with District.

Duration Setting

Non-Employee User ID Expiration - Every user ID established for a non-employee must have a specified expiration date. Accounts will not be created without an end date.

Changes and Maintenance

User Status Changes - Every user must notify the Systems Administration Unit about changes in their status with District.

Inactive Account Maintenance - All inactive accounts over 90 days old must be either removed or disabled.

Number Of Privileged User IDs - The number of privileged user IDs must be strictly limited to those individuals who absolutely must have such privileges for authorized business purposes.

VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. District reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. District does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, District reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

DEFINITIONS

Account (User ID or Username) – A unique string of characters assigned to a user by which a person is identified to a computer system or network. A user commonly must enter both a user ID and a password as an authentication mechanism during the logon process.

Confidential Information (Sensitive Information) – Any District information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, student names and personal information, employee salaries, skills, positions, organizational charts and organization information such as financial results, product costs, and pricing. Confidential Information also includes any confidential information received by District from a third party under a non-disclosure agreement.

Contractor – Any non-employee of District who is contractually bound to provide some form of service to District.

Password – An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

System Privileges – Advanced powers or authorities within a computer system, which are significantly greater than those available to the majority of users. Such persons will include, for example, the system administrator and network administrator who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the access rights of existing users.

User - Any District employee or partner who has been authorized to access any District electronic information resource.

REFERENCES

ISO/IEC 27002 – 11 Access Control

Employee Notification Forms

The SSCSD uses an electronic/web portal to report and document the creation and/or changes in user accounts.

SARATOGA SPRINGS CSD : PERSONNEL DEVELOPMENT : EMPLOYEE NOTIFICATION FORMS

Home

My Classes & Shortcuts

My Content

My Account

Tools

EMPLOYEE NOTIFICATION FORMS

 **Incoming SUBSTITUTE Notification**

Use this form to notify the IT Department of any Incoming substitute personnel (teacher, aide, clerk, monitor, secretary, other) who need IT accounts.

 **EXITING Employee Notification Form**

Use this form when any employee leaves the district.

 **CURRENT Employee Account Adjustment Notification**

Please use this form to Notify IT of additional or removal of accounts for EXISTING (CURRENT) EMPLOYEES.

 **NEW Employee Notification**

This form is designed to obtain necessary data for account creation for NEW EMPLOYEES.

 **Incoming STUDENT TEACHER Notification/Account Creation**

Use this form to notify IT and Guidance Staff of the need for IT accounts and schedule for STUDENT TEACHERS.

- **(pp.7 – 8)** *The Program Coordinator is responsible for adding and deactivating staff user accounts in the System, however, anyone with the super-user permissions (32 users) can add and deactivate staff user accounts.*

* (p.8) For example, an employee of the NERIC, which provides IT support for the District, would be included in a user group with heightened permissions. However, NERIC employees do not need grade modification privileges

* (p.8) For example, an IT staff person made 183 student grade changes but could not provide any written documentation supporting the basis for the changes. This user indicated she assisted staff that were not as familiar with the System.

User Access

We agree that the number of users who have elevated privileges can be reduced. The number listed in the audit report appears to be inflated as some members are counted multiple times as they exist in multiple groups.

See
Note 10
Page 24

Clarification is requested regarding the 27 active former user accounts that were tied to former employees. These accounts may have been listed in [REDACTED] but were disabled in the active directory which would not allow those users to login to the system.

See
Note 11
Page 24

Remote NERIC employees have never changed a grade (your findings support this), but need access to these areas for troubleshooting and support.

See
Note 12
Page 24

This IT staff member was assisting multiple teachers with these changes, and made no changes without teacher requests.

See
Note 13
Page 24

Assume Identity

- (p. 8) *District officials should strictly control the ability to grant or modify user rights in the System.*

We agree that the number of users who have elevated privileges can be reduced. The number listed in the audit report appears to be inflated as some members are counted multiple times as they exist in multiple groups.

See
Note 14
Page 24

Assume-account/identity feature is designed to let users with elevated privileges assumes the roles of users with less privileges to troubleshoot and verify data. It does not allow users with less privileges to assume the role of someone with elevated privileges.

See
Note 15
Page 25

The Student management system creates a log file when any user assumes the identity of another user. If a change is made in the assumed users name the change will tie back to the person who assumed the identity. Mr. Jones assumes the identity of Mrs. Smith. He makes a grade change for one of Mrs. Smith's students. The log file will demonstrate that Mr. Jones, assuming the identity of Mrs. Smith, made the change.

- (p. 9) *We found the district does not monitor audit logs or change reports. Despite having the ability to produce audit logs, the district did not generate audit logs or review them for potential unauthorized changes.*

District officials indicated that they would review audit logs only if an issue was brought to their attention. 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.

Audit logs

The district clarifies the statements below:

██████████ has the ability to produce an unlimited amount of logs see (diagram below) for any change for any user. The audit log tool in ██████████ does not flag "suspicious activity". The Saratoga Springs City School District Technology Department would not be able to identify unauthorized activity without a request. Though reviewing audit logs in ██████████ is time consuming and labor intensive, the District will review the logs for assume-identity and grade changes by non-teachers after the end of the school year once teacher verifications have taken place.

Response to Recommendations

1. The ability to make grade changes is already restricted to guidance counselors at the request of a teacher. The High School has already put in place a system for documenting changes as authorized by teachers.
2. The District will adopt policy regarding the use of the lock out function and would appreciate any guidance regarding best practice policies already in use.
3. The Program Coordinator II will produce an annual report reviewing when the lock out function was bypassed, by whom and for what reason.
4. The District will adopt policy regarding the grade change function and would appreciate any guidance regarding best practice policies already in use.
5. Written permissions will be crosschecked with systems users' reports on an annual basis.
6. After teacher verifications are completed each year, the Guidance Department Heads will submit an e-mail to the Program Coordinator II stating that all grade changes are completed for the year and the final grades can now be submitted to NYSED.
7. User access rights are currently under review and the rights will be limited based on the needs of carrying out the function of the position.
8. User permissions are currently under review and the rights will be limited based on the needs of carrying out the function of the position.
9. Outdated user accounts have been deactivated and there will be a review of user permissions on a quarterly basis.
10. The assume-identity feature is limited to counselors and super users and is only used to allow the authorized person to assist a teacher in expediting grade changes. The assume-account feature is limited to only the Super Users (which is the IT Staff, NERIC Staff, ██████████ Staff and a few select and trusted teachers who handle parent accounts) that use this function to actually become the end user to trouble shoot problems with that users account. This maintains the integrity of the passwords not being shared. As stated before, both the assume-identity and the assume account features identify the person making the changes rather than the account's owner and are ONLY used at the request of the end user for help with their account. Both of these features and the users that have this ability will be reviewed annually.
11. Though reviewing audit logs in ██████████ is time consuming and labor intensive, the District will review the logs for assume-identity and grade changes by non-teachers after the end of the school year once teacher verifications have taken place.
12. Current practices and procedures will be codified in policy and it would be appreciated if best practice policies already in use in other districts could be shared.

Thank you for the opportunity to respond to the findings of the Office of the State Comptroller's Access to Student Grading Systems examination. Feel free to contact me with any questions.

Sincerely,

Michael M. Piccirillo
Superintendent of Schools

Cc: Board of Education
Dave L'Hommedieu, Assistant Superintendent for IT and Operational Innovation
Kurt Jaeger, Assistant Superintendent for Business
Dr. Brett Miller, High School Principal
Doug Silvernell, Assistant Superintendent for 21st Century Teaching and Learning

APPENDIX B

OSC COMMENTS ON THE DISTRICT'S RESPONSE

Note 1

The term “District officials” is used to cover a broad range of titles succinctly. On page 4 of our report under the section “Lock Out Dates,” we identify the specific District officials who modified the lock out dates.

Note 2

The lock out function is an important System control specifically incorporated into the software for the purpose of preventing teacher grade changes after a date established by District officials. In the event that grade changes are necessary, the System provides other more restricted mechanisms to change grades after the lock out date, such as having users with heightened permissions make the changes after receiving appropriate and approved documentation. Bypassing the lock out date control increases the risk that inappropriate grade changes could be made.

Note 3

The term “District officials” is used to cover a broad range of titles succinctly. The “Grade Modifications” section of our report on page 5 notes that guidance counselors typically made the grade changes. We further note on page 8 that an IT staff person also made grade changes. In addition, our audit testing found that 61 percent of grade modifications made by users with heightened permissions could not be supported by written documentation. Due to the volume and timing of these undocumented changes, we believe our statement regarding “little or no oversight” is accurate.

Note 4

We used the descriptor “non-teachers” when summarizing findings in the report. The specific individuals who made the changes are documented throughout the body of the report. The word “routinely” is used to describe a procedure that District officials informed us was a longstanding practice for grades recorded initially at a failing 64. Our tests showed that, for such grades, the word “routinely” was accurate.

Note 5

We found 126 student grade changes between June 2013 and November 2014 that pertained to previous school years as far back as 2009-10. As it pertained to SED reporting, our testing found 59 separate instances where the grades submitted to SED were lower than the permanent grade record maintained by the District. Early SED cutoff dates were not the only reason for these discrepancies. However, we modified the language in our report to say, “These grade changes have resulted in grades being under-reported to the State Education Department.”

Note 6

We modified the wording of our report to address this concern. The statement now reads, “These weaknesses jeopardize the integrity of the students’ grades and increase the risk that staff with appropriate System permission can inappropriately modify student grades.”

Note 7

The report states that 175 users (footnoted to explain that some users within these groups are assigned to more than one group) had the permissions requisite to make such changes. Our review of the District’s audit logs related to these grade changes found (page 8 – “User Access”) 21 of these users actually made grade changes.

Note 8

Our statement “the District does not adequately control grade changes” is supported by the fact that 175 users had the requisite system permissions to change grades and the changes that were made were not supported by written documentation 61 percent of the time.

Note 9

We concur that the Board adopted an information security policy manual. However, the District has not adopted written policies and procedures for adding users, establishing users’ access rights, deactivating or modifying user accounts, granting user permissions and monitoring user access.

Note 10

Our report contains footnote references indicating that users belong to multiple groups.

Note 11

We acknowledge that a user would also need access to the active directory to access a System account. However, best practice dictates that the System account be disabled.

Note 12

We removed the example of a NERIC IT employee not needing such rights in the report.

Note 13

District officials could not provide us with appropriate written authorization by a teacher supporting these changes. Therefore, this statement cannot be confirmed.

Note 14

We added footnote #6 to address this concern.

Note 15

A user with assume account permissions may assume the account of any other user, including users with elevated privileges.

APPENDIX C

AUDIT METHODOLOGY AND STANDARDS

We reviewed access to the District's Student Grading System for the period July 1, 2013 through November 30, 2014.

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 NERIC staff, to gain an understanding of the District's student grading application and authorized users; assignment and monitoring of user access rights; and IT policies and procedures.
- We compared a list of current active employees to a list of current System staff users to determine if any System users 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 System 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 System users to verify they were no longer active System users.
- We obtained a listing of user groups and reviewed permissions granted to each user group to identify permissions considered incompatible with assigned job duties.
- We selected a judgmental sample of 10 grade changes made by users with teacher permissions, selected from System audit logs, to determine whether the teacher had made the change. We focused our testing on changes made to grades for marking periods that had already been closed out, fail to pass changes, and changes made for different courses.
- We selected a judgmental sample of 90 grade changes made by users with counseling permissions, selected from System audit logs, and determined whether these grade changes were authorized, documented and supported. We focused our testing on changes made to final grades for marking periods that had already been closed out, fail to pass changes, and changes made for different courses.
- We judgmentally selected 10 final student grades and determined whether they agreed with teacher-prepared grade books for the 2013-14 school year.
- We compared final grades submitted to SED with the appropriate legacy grades currently reported by the System. We reviewed discrepancies.

- We judgmentally selected five parent and five student users to verify the individual user (and the parent/student group) had just view-only rights. We obtained the parent user list and judgmentally selected an on-site staff person who was a parent.
- We obtained a listing of children enrolled in the District who were related to influential District officials including District administrators, principals, counselors and Board members. We determined that District officials had students as children in the District. We reviewed grade changes, if any, associated with these students to determine whether such changes were appropriately authorized and documented.
- We reviewed the audit logs and analyzed trends to determine items for further testing.

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.