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

Dr. Brendan Lyons, Ed. D.
Superintendent
Arlington Central School District
144 Todd Hill Road
LaGrangeville, New York 12540

Report Number: S9-15-47

Dear Dr. Lyons 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 Arlington 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 grade book systems for the period July 1, 2013 through March 3, 2015. 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. 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 plan to initiate corrective action. 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). 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 13 percent of the time.

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 Towns of Beekman, East Fishkill, Hyde Park, LaGrange, Pawling, Pleasant Valley, Poughkeepsie, Union Vale and Wappinger in Duchess County. The District operates 11 schools (four elementary, two primary, two intermediate, two middle and one high school) with approximately 9,000 students and 1,500 employees. The District's budgeted appropriations totaled $191.1 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 Director of Data Services 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 at the Mid-Hudson Regional Information Center (MHRIC), which 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 students, parents, teachers, administrators and various other District staff, as well as MHRIC employees and the vendor, who are involved in supporting the System. The District assigns access permissions for the 8,300 users[1] in its System through 48 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. Specifically, we found that grade changes made by non-teachers after the marking periods had closed lacked documentation to support the changes 13 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 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.

[1] The District has 48 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.

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 registrars and principals set 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 22 users including six District user accounts, 15 MHRIC employees and one software vendor account. The District user accounts included two registrars, two information technology (IT) department staff and two generic staff accounts. 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 generally uses the lock out function to restrict grade modifications; however, improvements are available. Specifically, we found the High School Registrar modified the established lock out date five times during the 2013-14 school year. Further, a member of the IT department staff had inadvertently modified the established lock out date while intending to modify an elementary school date. The High School Registrar stated that she will not change the lock out date without the school principal's approval. The District has no written documentation to support this representation. During the audit period, there were 136,697 grade modifications made by teachers; 1,614 modifications (1 percent) took place after the initially established lock out dates. Board and management established policies and procedures, with appropriate compliance monitoring, will strengthen the District's controls over the lock out function and associated grade modifications.

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 13 percent of the time. These modifications generally included changing grades from failing to passing and increasing grades

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

(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 permissions[4] must make grade changes after the close of a marking period. During our audit period, high school teachers and heightened permission users made 136,697 grade changes. The user group with heightened permissions made 4,416 of these changes. We tested 90 grade changes[5] made by this user group (typically registrars) and found that 12 (13 percent) could not be supported with written documentation from the teacher, or other appropriate individual, authorizing the change. Nine of these unsupported changes (75 percent) changed a grade from failing to passing and three changes (25 percent) increased a grade.

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

- In January 2014, a Career and Financial Management grade was changed from a 37 to 67 for the first marking period of the 2013-14 school year. The registrar could not provide an explanation for the change.

- In May 2014, a United States History grade was changed from a 48 to 65 for the second marking period of the 2013-14 school year. The registrar could not provide an explanation for the change.

- In June 2014, an Economics grade was changed from a 63 to 65 for the fourth marking period of the 2013-14 school year. The registrar could not provide an explanation for the change.

Prior-Year Grade Changes – We reviewed the System log of grade changes made by users with heightened permissions. We found they made 408 student grade changes between June 2013 and February 2015 that pertained to previous school years as far back as 2008-09. We judgmentally selected and tested five prior year grade changes and found one related to the 2008-09 school year, two related to the 2010-11 school year, and two related to the 2011-12 school year. For example:

- In July 2013, a grade for a General Science course taken in the 2010-11 school year was changed from a none to 95 based on a transcript, obtained from the student's prior school, in support of the modification.

- In October 2013, a grade for a Biology course taken in the 2010-11 school year was changed from a none to 84 based on an unsigned "New Student Transcript Information" sheet generated by the school's guidance department.

[4] For testing purposes, we did not test grade changes made by teachers during the marking period.
[5] See Appendix B, Audit Methodology and Standards, for details on our sample selection.

Further, registrar-level officials were unable to provide an explanation for three of these prior year grade changes.

Registrar-level officials explained that these changes occur as the result of teachers specifically asking them to make the changes; however, these authorizations are occasionally verbal and undocumented. 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 84,172 grades. We found seven 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 90 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 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 requesting access rights be assigned to new employees based on the job for which the employees have been hired. The IT Department will assign the employee to a 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 are 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 Director of Data Services is responsible for adding and deactivating staff user accounts in the System; however, anyone with the super-user permissions (18 users) can add and deactivate staff user accounts. Further, we found 22 users with the ability to modify student grades at any point during the school year. These users include six District user accounts, 15 MHRIC

employees and one software vendor account. The District user accounts included two registrars, two IT department staff and two generic staff accounts. We found that the two generic staff accounts had not logged onto the system and had not modified student grades at any time during our audit period. The District's Director of Data Services could not determine why or when the accounts were created and, accordingly, disabled the accounts. Further, we found that only five 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. For example, the 15 employees of MHRIC and the one user account for the software vendor that provides IT support for the District would be included in a user group with heightened permissions. However, these users do not need grade modification privileges.

We also found two generic accounts being used by MHRIC and District software vendor staff to access the System. These accounts provide powerful system rights/permissions with no accountability as to any work performed while logged onto the System as a generic user.

Further, we found that the System contains active user accounts for 23 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.

- The assume-account feature is similar to the assume-identity feature in that it allows the user to access the System for students assigned to the user whose identity they assume. However, it also allows a user to inherit all the given rights/permissions of that user.

During our testing, we identified 18 users, in two user groups, with the ability to assume-identity and assume-account permissions of another user. In total, these two user groups (containing two staff users, 15 MHRIC employees and one System vendor employee) can perform the assume-identity or assume-account function.

While our audit testing of grade changes (by these users), enabled by the use of the assume identity or assume account permissions, found no unauthorized changes, the potential exists that users so enabled could undermine the integrity of the grading system. Accordingly, the District should restrict the granting of such permissions wherever feasible and monitor, on a periodic basis, the use of permissions granted.

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. Adopt policy guidance regarding the utilization of the lock out function including written authorizations required and what procedures must be followed to bypass this control.

2. Periodically review the bypassing of the lock out function and determine the appropriateness of the changes.

3. Adopt policy guidance relating to the procedures and requirements for making grade changes in the current year and for prior years.

4. Periodically review the grade changes made by the heightened permission users and determine the appropriateness of the grade changes.

5. Update the annual reporting to the State Education Department to ensure accurate grade records are being reported.

6. 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.

7. 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.

8. Review current user permissions and deactivate inactive users from the System.

9. Consider whether the assume-identity and assume-account features are appropriate for use. If District officials decide to use these features, they should work with the System vendor to determine if the audit log report format can be modified to clearly show user activity performed and all accounts involved when these features are used.

10. Periodically review available audit logs for unusual or inappropriate activity.

The Board should:

11. 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 Arlington Central 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 page.

ARLINGTON CENTRAL SCHOOL DISTRICT

PHILIP BENANTE, DEPUTY SUPERINTENDENT

144 Todd Hill Road • LaGrangeville, NY 12540

Voice 845-486-4460 • Fax 845-486-4457 • E-mail pbenante@acsdny.org

June 15, 2015

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

Dear Ms. Singer:

I am in receipt of the Office of the State Comptroller's draft findings report that was sent to our district on May 27, 2015. Subsequently, I participated in a debrief meeting with you and [redacted] on June 2, 2015, along with representatives of the Arlington Central School District.

I have found no factual errors present in the draft report. The report establishes that a verification process needs to be established for when a teacher makes a grade change to memorialize that a building principal has authorized such a change as having merit. Additionally, the report includes recommendations that will make our student grade management system even stronger through the establishment of policy and procedures that further guide the student grade system.

However, the report does not capture the current strengths that exist within our system. Specifically, we believe that the current limitations on the access to the grading portal for grade changes is a noted strength of our student grade system. Access is limited to the classroom teachers and the registrar and is not available to building administrators or guidance counselors. Currently, our teachers verify course grades with our building administrators at the close of a course to discuss any issues or concerns for student grades. Finally, written verification is in place for most grade changes. We look forward to taking steps to make sure that procedures are in place next school year to ensure that written verification will be in place for all grade changes.

On behalf of our school district, I would like to thank you and your team for meeting with us over the past three months. We found the audit process to be informative, and look forward to strengthening our processes and procedures related to the student grade system.

Respectfully,

Philip Benante
Deputy Superintendent

Cc: Brendan Lyons, Superintendent of Schools
Board of Education

Our mission is to empower all students to be self-directed, lifelong learners, who willingly contribute to their community and lead passionate, purposeful lives.

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

We reviewed access to the District's Student Grading System for the period July 1, 2013 through March 3, 2015.

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.