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

Brett Provenzano
Superintendent of Schools
Fairport Central School District
38 West Church Street
Fairport, New York 14450

Report Number: S9-15-48

Dear Mr. Provenzano 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 Fairport 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 18, 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 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. 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. The District has a process to document grade changes; however, these documents are destroyed at the end of each school year and no documentation exists to support grade changes. We found that grade changes made by non-teachers after the marking periods had closed lacked documentation to support the changes 70 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 Town of Perinton in Monroe County. The District operates eight schools (four elementary, one 9th grade, two middle and one high school) with approximately 6,300 students and 2,000 employees. The District's budgeted appropriations totaled $110.6 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 seven-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 headed by the Director 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 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 the System's software vendor, who is involved in supporting the System. The District assigns access permissions for the 9,900 users[1] in its System through 78 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 70 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.

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

[1] The District has 78 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.

period when grades are to become final and entered into the System. The District's 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 16 users including 10 District user accounts and six software vendor accounts. The District user accounts included two registrars, three guidance department staff and five information technology (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 generally uses the lock out function to restrict grade modifications. However, improvement opportunities are available. Specifically, we found the High School Registrar modified the established lock out date nine times during the 2013-14 school year. The High School Registrar stated that she will not change the lock out date without the approval of the school principal. The District had no written documentation in support of this representation. During the audit period, there were 93,545 grade modifications made by teachers; 1,526 modifications (2 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 potential 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). The District has documentation requirements to support grade changes in the high school. This process requires teachers to provide the registrar with a completed "Grade Correction Form" prior to the registrar making the grade change.

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 70 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. The design of the documentation requirements is a good control; however, it is not consistently applied across the schools in the District. Further, compliance is not monitored.

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

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 96,478 grade changes. The user group with heightened permissions made 2,933 of these changes. We tested 90 grade changes[5] made by this user group (typically registrars) and found that 63 (70 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 39 (62 percent) changed a grade from failing to passing; 21 (33 percent) increased a grade; and three (5 percent) decreased a grade.

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

- In May 2014, an English grade was changed from a 62 to 84 for the 2013-14 school year.
- In April 2014, a Biology grade was changed from a 62 to 73 for the 2013-14 school year.
- In December 2013, a Health grade was changed from a 55 to 65 for the 2013-14 school year.

Due to the lack of policy guidance, registrar-level staff are changing grades from failing to passing without any documentation and authorization from the teacher. The District has a process for documenting grade changes. However, the District destroyed written documentation in support of grade modifications upon the start of a new school year. Therefore, support for grade changes was not available for review.

Prior-Year Grade Changes – We reviewed the System log of grade changes made by users with heightened permissions. We found they made 383 student grade changes between June 2013 and March 2015 that pertained to previous school years as far back as 2007-08. We judgmentally selected and tested 10 prior-year grade changes and found two were related to the 2009-10 school year; one related to the 2010-11 school year, two related to the 2011-12 school year, and five related to the 2012-13 school year. For example:

- In July 2013, a grade for a Chemistry course taken in the 2012-13 school year was changed from a 58 to a 74.
- In May 2014, a grade for a Biology course taken in the 2012-13 school year was changed from a 63 to a 65.

Due to the unofficial practice of destroying written documentation in support of grade modifications pertaining to prior school years, no documentation exists as to the basis or necessity of these modifications.

[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.

Further, 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 61,404 grades. We found 12 separate instances where the grades submitted to SED differed from the permanent grade record maintained by the District. One grade on the SED report was three points lower than the grade maintained by the District, the SED report had three grades not maintained by the District, and the District maintained eight grades not listed in the SED report.

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 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 Manager of Student Information Systems is responsible for adding and deactivating staff user accounts in the System; however, anyone with the super-user permissions (eight users) can add and deactivate staff user accounts. Further, we found 26 users with the ability to modify student grades at any point during the school year. These users include District IT staff, registrars and counselors (this group generally does not include teachers). However, we found that

only 12 of these users actually made grade modifications. IT staff attribute the number of users that have not made grade changes to two user groups that include a bundle of heightened permissions. For example, 15 members of the District's counseling staff have heightened permissions, but none of its members made more than 2 percent of the total number of grade changes. Additionally, six employees of the District's software vendor, which provides IT support, are included in a user group with heightened permissions. However, these vendor employees do not need grade modification privileges. By inappropriately granting users the ability to change grades, the District increases the risk of unauthorized grade changes being made.

We also found that the System contains active user accounts for 42 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 16 users in three user groups with the ability to assume identities of another user. In total, these six user groups (containing 10 staff users and six System vendor employees) can perform this assume-identity function.

- 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. We identified eight users who have the ability to assume the account of another user. These eight users are in one user group (containing two staff users and six System vendor employees) who can perform this powerful function.

While our 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. Retain grade modification documentation.

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. 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.

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 Fairport 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 pages.

Quality Learning & Caring...

FAIRPORT CENTRAL SCHOOL DISTRICT

Brett Provenzano
Superintendent of Schools

38 W. Church Street, Fairport, New York 14450
585-421-2004 • FAX 585-421-3421
bprovenzano@fairport.org

July 13, 2015

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

Re: Fairport Central School District's Audit of Student Information System Response

Dear Ms. Singer,

Below please find Fairport's written response regarding the Comptroller's audit findings from June 4, 2015 and exit discussion from June 11, 2015.

Fairport's Written Response to Comptroller's Audit Findings on 6/4/15 and Exit Discussion on 6/11/15
Submitted by William C. Cala, Ed.D.

The New York State Comptroller student information system audit for Fairport School district was broken down into two major categories; grade changes and controlling access to the system. The process reaffirmed many of the strengths from which we control and manage our system along with ways we can improve. The data review and system discoveries that this audit performed emphasized our need to define policy and document grade change processes. We take pride in the results that show stringent controls are in place.

We are in agreement with recommendations 1-6 and will implement the suggestions. The audit defined that areas of improvement center around creating further policies that define the rules behind specific processes within the student information system. We will create policies and documentation that define retention periods for grade change documentation. We will also create policies that define approval path requirements for grade changes.

We are not in agreement with the audit conclusions 7-12. We consistently monitor audit logs, evaluate user's rights and access. Many of our processes and system enhancements such as Account Assume have been developed by the student information system vendor in response to our need to securely and efficiently manage and monitor the system. We believe our control of and use of these features has been demonstrated as to not compromising the integrity of our systems.

- We strongly support that our use of super-user privilege and assume-identity system features is appropriate and does not jeopardize integrity. The assume-identity feature is used to troubleshoot and support day-to-day technical issues and is given to only those in need to perform their job role.

See Note 1 Page 14

- We believe there is no evidence that the 26 super-user accounts cited in this report is an indicator of inadequate access controls. Many of these super-user accounts are limited to only the specific building the staff member works in. Guidance counselors, administrative workers, and support personnel play an integral role in managing the many day-to-day needs that rely on heightened building level access. We believe this is a very limited number considering our district size of 6100+ students and 1000+ instructional staff.

See Note 2 Page 14

- We have also implemented best practice controls by utilizing 72 security group structures that strictly limit information access to the job role and location.

- We have an interactive and synchronized staff directory that provides a live view of current job roles and security groups. This creates an interactive layer of checks and balances.

- The audit inaccurately cited us for having 42 former employee accounts reported as having access to the student information system. An additional security layer protected 37 of the 42 accounts. The 37 accounts were previously deactivated from the main district authentication system which eliminates all access to any of our connected systems, including the student information system.

See Note 3 Page 14

- Our centralized access authentication system lies at the heart of all of our systems. Changes are made in the main system and then flow through or affect the others. Our staff directory, staff file servers, computer, email access, and student information systems are aligned and connected on a nightly basis.

- Prior to this audit a process was created (Spring 2015) that deactivates inactive users after 60 days.

- The audit cited 93,545 grade changes. This statistic is misrepresented as 88,000 of these changes reflect initial grade entry and not grade changes. We contacted the vendor and reviewed the reports the auditors referenced and found that the system defined an initial grade entry as a "Mod" where it should be an "Add". We have since asked the vendor to update the report field to accurately describe the action.

See Note 4 Page 14

- Our collaborative account management system has been in place for over 4 years which documents account access changes. Email notifications connect all parties involved anytime a change is made. The HR and IT team organize, manage and document account activity in this system.

Included in the Scope of this audit, but completely missing from the findings of this report, was the specific targeting of grades and grade changes of students related to district administrative staff and board members. When inquiries were made as to why the Auditors targeted these student grades specifically, the response given cited the potential pressure placed upon teachers to change grades inappropriately by officials in positions of authority. While we agree this risk exists, we must assume by completely eliminating any discussion from the Audit Report findings that the Auditors found no abuse in any of the districts. As it is the Comptroller's responsibility to promote good governance, we believe this finding should be highlighted in order to build confidence in the communities in their public officials and the associated tax dollars used in support of education.

See Note 5 Page 14

However, the specific targeting of students related to district administrative officials calls forth serious concerns that should also be addressed. Specifically, several Fairport Board of Education members became concerned when finding out unofficially through their children and teachers that auditors had specifically made inquiries to teachers about their grades. Having learned this, board members sought to better understand the purpose of such inquiries, how the inquiries were conducted and what has become of the information. During this process, we found the following to be of most serious concern in how the auditors conducted themselves in this effort.

- When auditors were specifically asked about the process, the board member asking the question was informed that only Super-Users were interviewed. This response however was inaccurate and potentially misleading in that evidence had been provided that a teacher reported to their union representatives regarding specific interviews targeting specific children of board members with specific accusatory questions of whether inappropriate request had been made. Such questions were not based on evidence, but simply based on auditor's perception that the possibility existed.

See Note 6 Page 14

- This mismatch in what the Auditors said occurred and what actually occurred provides concerns and calls into question integrity of findings of the report. The Comptroller's office should have hyper-sensitivity in the way it conducts itself considering its mission to promote good governance.

See Note 7 Page 15

- We recognize and agree that the potential risk exists for those in administrative or elected positions to inappropriately use influence to alter outcomes. However, we have concerns in the way the Auditors pursued this line of inquiry. Auditors made no effort to mask and protect individual identity or information. That auditors took specific names, rather than request aliases for students. Auditors did not look for irregularities, but rather targeted students, specific grades and the associated teachers.

  One specific example where an irregularity existed that accounted for such a change. A teacher had been asked by the auditor if a board member had unduly pressured them to alter a grade. Citing an example, "discovered" that a grade had been changed from 0 to the different grade during the course of the week. Upon further investigation, which the auditors themselves should have done, it was discovered that 100% of the students in the associated class had their grades changed from 0 to the appropriate grade for each student. The inquiry to the teacher, indeed the entire effort, could have been avoided had the Auditors used aliases with students and done appropriate audits of the grades and learned that all grades had been submitted as new and not as a modification. The specific targeting and questioning of students without first searching for irregularities in the overall population calls into question the real purpose of the effort.

See Note 8 Page 15

- The Comptroller's office should have hyper-sensitivity in how it conducts itself in order to provide confidence and integrity in the reports issued. In order to avoid the appearance of targeting students and specific individuals of leadership, the auditors should engage methodology that allows them to see if irregularities exist before pursuing further inquiries.

See Note 8 Page 15

- One final related concern is specific to the privacy of our children. In the current and dynamic environment, privacy and data protection are of the utmost concern. Parents maintain the ultimate responsibility to protect and preserve their child(ren)'s privacy. It is concerning that parents where not formally notified that their child(ren)'s grades/other information were being closely scrutinized. The Comptroller's office should recognize the rights and concerns of parents and take appropriate action so as not to call into question the intent of its objectives.

See Note 9 Page 15

- FERPA requires any information be completely removed from Comptroller system upon completion of the audit. We request and believe the Comptroller's office should provide assurances that it complies with this law; that student data has indeed been expunged from the system, insuring the privacy of students and their families.

Fairport Schools has demonstrated proper design and maintained access controls at a very high level. We recognize and will improve our documentation and create formal policies. We feel it is a disservice to the public and community to categorize the entirety of our work specific to controlling access as "inadequate". We have demonstrated that the student information system is protected and viewable by only those that need to perform the job role at hand. We will continue to work with the vendors of all of our information systems to take advantage of the protections that data system alignment affords.

Sincerely,

Brett Provenzano
Superintendent of Schools

APPENDIX B

OSC COMMENTS ON THE DISTRICT'S RESPONSE

Note 1

Our report states "the District should restrict the granting of such permissions wherever feasible and monitor, on a periodic basis, the use of permissions granted." We did not say too many users have these privileges. District officials, however, were not monitoring these permissions, which can jeopardize integrity.

Note 2

As our report states, only 12 of the 26 users who have super-user privileges actually made changes during the scope period. Therefore, many of the 14 who did not make changes likely do not need these privileges.

Note 3

Our audit found 42 former users with active accounts in the System. While it is accurate that a user who does not also have network access could not access their System account, best practice would warrant these accounts being deleted or made inactive.

Note 4

Our report included what the District's System reports in its audit logs.

Note 5

Our audit did not solely target the grades of students related to District administrative staff and Board members. Instead, we identified grade changes associated with these potentially higher risk students and selected them for audit testing to determine whether they were appropriately authorized and documented. We did so in the same manner as the testing we performed on the other students selected for testing. Our testing in this area did not result in a finding and, accordingly, was not reported upon in the body of the report. However, we appropriately documented our audit testing in Appendix B.

Note 6

It appears that there was a misunderstanding between the Board member and the auditors regarding the explanation of the process. Our audit interviews asked about grade changes made by teachers and heightened permission users. We made no accusations. Rather, we inquired as to whether the users had been asked to make such grade changes by anyone other than the student's teacher.

Note 7

There was no mismatch between what we said and what occurred. OSC conducts its audits with transparency and integrity following generally accepted government auditing standards. It was appropriate for the audit to include testing for higher risk grade changes.

Note 8

Due to the nature of this audit test, it was not possible to "mask" the identities of the students involved. Further, OSC has instituted various procedures and reviews to ensure that the audit complies with all laws and regulations regarding confidentiality. Our audit procedures are designed to select, in this case, higher risk items of the total population for audit testing to determine if "irregularities" exist rather than "targeted students, specific grades and the associated teachers." Our audit tests were not designed to determine trends or similarities to other grade changes. Instead, we selected items from the total grade change population, as defined by the District's System, for audit testing. The purpose of the audit is as expressed in our report.

Note 9

As with all of our audits, OSC considers it to be vitally important to protect potentially confidential and sensitive information. We complied with all applicable laws and OSC policies when maintaining confidentiality during the conduct of our audit. Our actions were appropriate and the intent of our objectives was transparent.

APPENDIX C

AUDIT METHODOLOGY AND STANDARDS

We reviewed access to the District's Student Grading System for the period July 1, 2013 through March 18, 2015.

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

- We interviewed District officials and 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.