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. Kishore Kuncham
Superintendent of Schools
Freeport Union Free School District
235 North Ocean Avenue
Freeport, New York 11520

Report Number: S9-15-46

Dear Dr. Kuncham 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 Freeport Union Free 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 February 12, 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). 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 26 percent of the time. In addition, these grade changes 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.

Background and Methodology

The District is located in the Town of Hempstead in Nassau County. The District operates eight schools (five elementary, one intermediate, one middle and one high school) with approximately 6,700 students and 2,000 employees. The District's budgeted appropriations totaled $156.4 million for the 2013-14 fiscal year. These costs are funded primarily through State aid and real property taxes.

The District is governed by a five-member Board 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 Executive Director for Operations 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 Nassau Board of Cooperative Educational Services (BOCES) 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 BOCES employees and the vendor, who are involved in supporting the System. The District assigns access permissions for the 3,500 users[1] in its System through 20 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 lockout 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 26 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 20 different active user groups, some of which include administrators, census, counseling, faculty, parents, teachers 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 Assistant High School Principal sets these dates before the start of each school year based on student report card reporting dates. Changes subsequent to this date are made at the high school by the programming office clerk upon authorization of the Assistant High School Principal and High School Principal. 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. Management provided these permissions to 10 District officials including nine guidance counselors and an IT department staff member. Further, management provided these permissions to seven IT consultants. 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 programming office clerk modified the established high school lock out date 10 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 77,613 grade modifications made by teachers; 2,592 modifications (3 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 three times, extending the original November 15, 2013 as late as the end of the school year (June 27, 2014);

- The lock out dates for the second and third marking periods in 2013-14, originally established at February 5, 2014 and April 28, 2014, respectively, were changed six 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 once, which extended the marking period from June 27 to July 1, 2014.

District officials indicated, due primarily to the District requirement that teacher grade books correspond to legacy grades, it is necessary for teachers to input grades after the initial lock out date on a regular basis. Accordingly, grade modifications occurred well beyond the initially established lock out date and an important system timeline control was bypassed. By allowing staff to circumvent established controls, the risk that unauthorized grade modifications could occur and go undetected is greatly increased. Current lock out date controls require users with heightened permissions to make the changes (programming office clerk) upon authorization of the Assistant

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

High School Principal and High School Principal. However, no written authorization was maintained.

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 26 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 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 79,534 grade changes. The user group with heightened permissions made 1,921 of these changes. We tested 90 grade changes[5] made by this user group and found that 23 (26 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 12 (52 percent) changed a no grade to 65 or better, one change (4 percent) increased a grade, and 10 changes (44 percent) modified a grade from failing to passing.

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

- In July 2014, an Economics grade was changed from a 38 to 66 for the 2013-14 school year. The counselor indicated a teacher had called and requested the change. The high school office programming clerk was unable to produce written documentation in support of this change.

- In June 2014, a Geometry grade was changed from a 50 to 65 for the 2013-14 school year. The high school office programming clerk was unable to produce written documentation in support of this change.

[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.

- In May 2014, an Algebra II/Trigonometry grade was changed from a 55 to 65 for the 2013-14 school year. The high school office programming clerk was unable to produce written documentation in support of this change.

<u>Prior-Year Grade Changes</u> – We reviewed the System log of grade changes made by users with heightened permissions. We found they made 40 student grade changes between June 2013 and March 2015 that pertained to previous school years as far back as 2010-11. We judgmentally selected and tested five prior-year grade changes and found one was related to the 2010-11 school year, one related to the 2011-12 school year, and three 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 60 to 65. The registrar stated that she changed the grade based on an authorization from the High School Principal. However, no documentation was available to support the change.

- In June 2014, a grade for a Math course taken in the 2012-13 school year was changed from a no grade to 98. The registrar stated that she changed the grade based on an authorization from an Assistant Principal, but the transaction was not documented by a signed authorization from the Assistant Principal.

Further, registrar-level officials were unable to provide an explanation for two 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 63,455 grades. We found 19 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 17 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.

<u>Policies and Procedures</u> – 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 informing the IT Department of the new hires. 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 District's Data Processing Consultant is responsible for adding and deactivating staff user accounts in the System; however, anyone with the super-user permissions (36 users) can add and deactivate staff user accounts. Further, we found 79 users[6] with the ability to modify student grades at any point during the school year. These users include counselors, District IT staff and various District data processing consultants. However, we found that only five of these users actually made grade modifications. Six of the users, having heightened permissions, but not having made grade changes, are data processing consultants affiliated with Nassau BOCES (five users) and a software vendor (one user). These data processing consultants 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 127[7] former District employees or individuals no longer associated with the District. For example, we found users that had resigned as far back as 2002. In addition, we found 14 generic user accounts; these cannot be traced to a specific end user. These former employees' accounts remained active due to a lack of awareness and monitoring. District IT staff stated that they are not notified of an employee's retirement or other separation from the District and the need to deactivate the applicable account.

Subsequent to fieldwork, the District reevaluated users' permission requirements and removed users from groups having the permissions needed to modify grades. Specifically, 35 users were removed from the "Super User" group, eight users from the "Counseling3" group and 21 from the "Administrators" group. During the scope period, 16 users made grade modifications. We included grade change transactions made by these users in our review of grade changes in the audit log and determined that changes were made consistent with assigned permission rights.

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

[6] Some users within these groups are assigned to more than one group.
[7] Sixty-nine users were not assigned to a user group, which limits their ability to access the System.

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 130 users in five user groups with the ability to assume identities of another user. In total, these five user groups (containing 123 staff users, five BOCES employees, one Data processing consultant and one System vendor employee) 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 seven users who have the ability to assume the account of another user. These seven users are in one user group (containing five BOCES employees, one data processing consultant and one System vendor employee) who can perform this powerful 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. 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 Freeport Union Free 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. District officials attached copies of updated procedures to their response. As their response letter included sufficient information to indicate their intentions, we did not include the attachments as a part of the final report.

Freeport Public Schools

235 North Ocean Avenue • Freeport, New York 11520 • 516-867-5200

Kishore Kuncham, Ed.D.
Superintendent of Schools

e-mail address:
kkuncham@freeportschools.org

Phone (516) 867-5205
Fax (516) 623-4759

June 5, 2015

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

Dear Ms. Singer,

This letter is the written audit response of the Freeport Public School District to your draft report of the audit your office conducted this spring. We have reviewed the draft report and we are enclosing our Corrective Action Plan(CAP) as required. The recommendations made in the draft report are already being addressed and, in fact, many of the steps in our draft corrective action plan began during the audit window, and this was acknowledged by your audit team. The audit team sent from your office was courteous, professional, and helpful.

New York State has not issued any regulations or guidance documents relating to District practices in the areas of Student Information System data access and permissions. While we did have procedures and controls in place, this audit has provided our District the opportunity to further review and strengthen policies and practices related to our Student Information System. Thus, the recommendations made by your office are helpful to us as we implement policies and practices that will strengthen our management of student information. We have implemented a documented approval process and audit trail for processing grade changes, have limited the "assume" functions, and updated administrative procedures for adding users, deactivating users, and for verifying that each user has only the level of access necessary for the performance of their job responsibilities.

We are pleased that your examination did not identify any data breaches nor any instances of non-compliance with federal or state statutes. The District places a high priority on student data security and has been guided by FERPA and our local Board Policies 5672, 6470, 7240, and7244 which address student records and data breaches. Policy number 5674 – Data Networks and Security Access, drafted last month by Erie BOCES, will be considered for implementation.

Sincerely,

Kishore Kuncham, Ed.D.
Superintendent of Schools

c. [redacted]
Mr. Michael Pomerico, President, Board of Education
Mr. Gerard Poole, Assistant Superintendent for Curriculum and Instruction
Mr. Michael Singleton, Executive Director for Operations

Freeport Public Schools

Audit of Student Information Systems

Corrective Action Plan

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.**

   Action Plan: No grade changes will be made without appropriate authorization and signatures. Any requests to make grade changes after the lockout date must be made in writing directly to an Assistant Principal or the Principal detailing the reason for the need to change, or record, a grade after the lockout date. If the administrator approves the "after lockout" change, he/she will forward the approval request to specifically designated building staff and direct them to make the authorized changes in the SIS. Only designated staff will have the system permissions required to enter grade changes. Any change thus entered must also be reflected in the teacher's physical grade book. Approval forms will be retained.

   Implementation Date: Policy/procedure modified and strengthened January, 2015

   Responsibility: Building Principals, Assistant Principals, and Data Administrator

2. **Adopt policy guidance regarding the utilization of the lock out function and what procedures must be followed to bypass this control.**

   Action Plan: Occasionally, based on extenuating circumstances such as weather, illness, network issues, etc., it may be necessary to change a lock date for the purpose of allowing teachers to enter grades. Changing lock dates can only be requested by building administrators. By default our SMS permits building schedulers the ability to change the configuration of marking periods, including lock date. This feature has now been disabled and this permission is available only to the Data Administrator and the Assistant Data Administrator. A building administrator who wishes to change a lock date must make a written request to the Data Administrator specifying the reason. The Data Administrator will retain a folder of such requests.

   Implementation Date: Immediate

   Responsibility: Building Principals, Assistant Principals, and Data Administrator

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

   Action Plan: Audit logs will be run between marking periods, and at random times, to monitor changes in lock dates and to review the rationale, documentation, and authorization for any such changes. The Assistant Superintendent for Curriculum and the Executive Director for Operations will review the audit logs as well as the folder of "lock date" requests from building administrators to determine whether any pattern or unusual activity is evident.

   Implementation Date: Immediate

   Responsibility: Assistant Superintendent, Executive Director for Operations, Data Administrator

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

   Action Plan: The District has adopted a procedure for implementing grade changes that reflects the current practice of requiring written authorization from a building administrator for any such change. The Grade Change authorization form has been modified and expanded to include a rationale for any requested change and provision for teacher assurance that the physical grade book has been revised to reflect the changed grade.

   Implementation Date: Immediate for current year changes, September 1, 2015 for prior year changes.

   Responsibility: Building Principals and Assistant Principals

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

   Action Plan: The Data Administrator will run audit logs between marking periods to monitor grade changes and to review the rationale, documentation, and authorization for any such changes. The Data Administrator will summarize that review and will forward that summary to the Assistant Superintendent for Curriculum and the Executive Director for Operations.

   Implementation Date: Immediate

   Responsibility: Assistant Superintendent, Executive Director for Operations, Data Administrator

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

   Action Plan: Grades cannot be changed at the state level after the year is locked in late August. In order to eliminate any opportunity for discrepancy, the Data Administrator will upload final grades to the SED just prior to the state's lock date in late August.

   Implementation Date: August 2015

   Responsibility: Data Administrator

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.**

   Action Plan: A procedure has been developed for assigning user rights and existing forms have been modified. The Human Resources Department will generate a New Employee form identifying the name and job title of any new employee. The form will be forwarded to the Data Processing Department where the Data Administrator will confer with the HR Department to determine the nature of the new employee's duties and will assign him or her to a permissions group with the minimum permissions compatible with those duties. All current users have had their access rights reviewed. Permissions for all security groups will be reviewed annually.

   Implementation Date: Already in effect

   Responsibility: Assistant Superintendent for Personnel, Data Administrator

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.

Action Plan: Security permissions for all users will be reviewed annually at the beginning of the school year with such review to be completed no later than October 31st. This review will focus on ensuring that permissions for all users do not exceed the requirements of their respective duties. That review has been completed this year and appropriate adjustments in permissions have been effectuated. Security permissions for all current groups have been reviewed to ensure that each group's permissions do not exceed those needed for the job responsibilities of those in the group. Any new security group must be authorized, and permissions defined, by Data Administrator in consultation with the Assistant Superintendent for Curriculum and the Executive Director for Operations.

Implementation Date: Already in effect

Responsibility: Assistant Superintendent for Curriculum, Executive Director for Operations, Data Administrator,

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

Action Plan: The Data Processing Supervisor will conduct periodic comparison of a list of all the District's active employees to a list of the current staff users of the SIS to determine if any users of the SIS are not District employees or if any former employees remain on the current user list. Accounts to be deactivated as needed. Staff members who are no longer with the district have had their accounts made inactive and all group associations have been deleted.

Implementation Date: Already in effect

Responsibility: Assistant Superintendent for Personnel, Data Administrator

10. Consider whether the assume-identity and assume-account features are appropriate for use.

Action Plan: The District has severely curtailed both "assume" functions. The "assume account" permission is available only to the System Administrator group and the "assume identity" permission is available to only the System Administrator group and four specific security groups created for the unique needs of a handful of users such as building principals.

Implementation Date: Already in effect

Responsibility: Assistant Superintendent for Curriculum, Data Administrator

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

Action Plan: An ongoing monitoring process will include the running of audit logs between marking periods to monitor grade changes or any unusual activity and to determine if any user's activity appears to exceed the level of access for which they are authorized. Users will be required to change passwords at least twice a year going forward, and passwords will be required to meet minimum strength requirements.

Implementation Date: Already in effect

Responsibility: Building Principals, Assistant Principals, Data Administrator

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.

Action Plan: Review and adoption of appropriate Board Policy and Regulations establishing requirements for implementation of effective measures to protect access to district networks to ensure the security of district data.

Implementation Date: Policy review currently in process.

Responsibility: Board of Education Policy Committee, Superintendent,
Central Office Administrators

NOTE: Implementation of the Corrective Action Plan will be overseen and monitored by the Assistant Superintendent for Curriculum and Instruction in coordination with the Executive Director for Operations.

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

We reviewed access to the District's Student Grading System for the period July 1, 2013 through February 12, 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.