



**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

Ms. Hillary Austin  
Superintendent of Schools  
Elmira City School District  
951 Hoffman Street  
Elmira, New York 14905

Report Number: S9-15-45

Dear Ms. Austin 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 Elmira City School District (District) in this audit. Within the scope of this audit, we examined the District's policies and procedures and reviewed access to the grade book systems for the period July 1, 2013 through January 8, 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 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 48 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 City of Elmira and Towns of Ashland, Baldwin, Big Flats, Chemung, Elmira, Erin, Horseheads, Southport and Caton in Chemung and Steuben Counties. The District operates 11 schools (eight elementary, two middle and one high school) with approximately 6,900 students and 1,100 employees. The District's budgeted appropriations totaled \$114 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 Technology Director,<sup>1</sup> 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 Greater Southern Tier Board of Cooperative Educational Services (GST BOCES), 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

---

<sup>1</sup> An employee of the Greater Southern Tier Board of Cooperative Educational Services fills this position. They are a contracted consultant for the District.

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 GST BOCES employees and the vendor, who are involved in supporting the System. The District assigns access permissions for the 3,600 users<sup>2</sup> in its System through 33 different user groups.<sup>3</sup>

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 48 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.

---

<sup>2</sup> The District has 33 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.

<sup>3</sup> 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 Director of Student Services, 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.<sup>4</sup> 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 15 users including 14 GST BOCES employees and one software vendor account. 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 a GST BOCES employee<sup>5</sup> modified the established lock out date three times during the 2013-14 school year. The GST BOCES employee stated that she will not change the lock out date without the registrar's representation that the school principal has approved the change. The District had no written documentation in support of this representation. During the audit period, there were 29,335 grade modifications made by teachers; only three modifications 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).

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 48 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.

---

<sup>4</sup> Generally, teachers do not have access to this level of user permissions.

<sup>5</sup> This individual is a GST BOCES employee under contract with the District for IT services.

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<sup>6</sup> must make grade changes after the close of a marking period. During our audit period, high school teachers and heightened permission users made 34,144 grade changes. The user group with heightened permissions made 4,809 of these changes. We tested 90 grade changes<sup>7</sup> made by this user group (typically registrars) and found that 43 (48 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 38 (88 percent) changed a no grade to 65 or better, two changes (5 percent) decreased a grade, and three changes (7 percent) modified a grade from failing to passing.

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

- In February 2014, a Geometry grade was changed from a 60 to 65 for the 2013-14 school year. The registrar could not provide any written documentation in support of the change from a failing to a passing grade.
- In July 2014, a final exam score was changed from a 52 to 98 for the 2013-14 school year. The registrar stated that she had been instructed to change the grade by the school principal but could not provide any written documentation in support of the change.
- In July 2014, a Health grade was changed from a 48 to 80 for the 2013-14 school year. The registrar indicated that a teacher had requested her to enter a grade for a student who had been ill, but she could not provide written documentation.

Prior-Year Grade Changes – We reviewed the System log of grade changes made by users with heightened permissions. We found they made 525 student grade changes between June 2013 and November 2014 that pertained to previous school years as far back as 2010-11. We judgmentally selected and tested 29 prior year grade changes and found two were related to the 2010-11 school year, three related to the 2011-12 school year, and 24 related to the 2012-13 school year. For example:

- In September 2013, a grade for an American Wildlife course taken in the 2012-13 school year was changed from a 64 to 65. According to the registrar, she was authorized by the principal to increase the student's grade because the student did extra work and deserved the increase in grade. However, there was no written authorization to support this grade change.
- In August 2013, a grade for a Global History course taken in the 2012-13 school year was changed from a 32 to 65 without any supporting documentation as to the basis or necessity of the modification. The registrar did not have any explanation for the grade change.

---

<sup>6</sup> For testing purposes, we did not test grade changes made by teachers during the marking period.

<sup>7</sup> See Appendix B, Audit Methodology and Standards, for details on our sample selection.

Further, the registrar was unable to provide an explanation for a total of 21 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 often verbal and are not documented. The failure to document approvals and the reasons for necessary student grade modifications increases the risk that such changes are not properly authorized and supported, which places the integrity of the student's permanent record at risk. For example, we reviewed the final grade report sent to SED for the 2013-14 school year, which contained 16,854 grades. We found 45 grades that did not match with SED. Specifically, there were 17 separate instances where the grades submitted to SED were lower than the permanent grade record maintained by the District and 28 grades were not reported to SED. Grades on the SED report ranged between one and 100 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 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, after approval, 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 Technology Director is responsible for adding and deactivating staff user accounts in the System; however, anyone with the super-user permissions (15 users) can add and

deactivate staff user accounts. Further, we found 19 users<sup>8</sup> with the ability to modify student grades at any point during the school year. These users include District IT staff, administrators, and registrars (this group generally does not include teachers). However, we found that only three of these users actually made grade modifications. IT staff attribute the number of users that have not made grade changes to general user groups that include a bundle of heightened permissions. For example, an employee of the GST BOCES, which provides IT support for the District, would be included in a user group with heightened permissions. However, GST BOCES employees do not need grade modification privileges.

We also found that the System contains active user accounts for 15 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 always 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. 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 15 users in one user group with the ability to assume identities of another user. This user group (containing 14 GST BOCES employees 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. The same users who have assume-identity rights/permissions in the District can perform this powerful function. These users do not have the capability to assign themselves additional user rights beyond those rights they have already been authorized.

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 using these permissions, 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.

---

<sup>8</sup> Some users within these groups are assigned to more than one group.

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.

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 Elmira City School District for the courtesies and cooperation extended to our auditors during this audit.

Sincerely,

Gabriel F. Deyo  
Deputy Comptroller

## **APPENDIX A**

### **RESPONSE FROM DISTRICT OFFICIALS**

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

# Elmira City School District



**Hillary J. Austin**  
Superintendent of Schools  
Administration Building  
951 Hoffman Street  
Elmira, NY 14905

Phone: (607) 735-3010  
Fax: (607) 735-3009  
haustin@elmiracityschools.com

June 5, 2015

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

Dear Ms. Singer:

On behalf of the Elmira City School District Board of Education, I would like thank you, your staff, and Comptroller DiNapoli for your thorough and complete examination of the management of the student grading information system used by our district. The auditors responsible for conducting the audit demonstrated professionalism throughout and we very much appreciate the thoughtful and respectful manner in which this audit was conducted.

Working through the audit process, we were able to examine our own systems, procedures, and protocols and through this experience with the auditors helped to confirm the areas of growth that we had identified. We have well-thought-out and diligent undocumented processes to manage the system to enter and change grades, but these processes need to be solidified into policy and regulations that provide district staff specific guidance for day to day operations to ensure the integrity of student grades. We have already begun to draft a Student Management System Policy to address this and with the guidance provided by the Comptroller's Office in the draft report, we will incorporate many of the recommendations into the final development of this policy.

Below are our responses to the recommendations contained in your audit report.

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.*

As noted by the auditors during the exit conference, the District maintains the appropriate tight controls over the changing of the lock out dates in the student grading system. We will be addressing this in the Student Management System Policy by specifying that overriding lock out dates will only be permitted with the approval of the Director of Student Services. This approval must be in writing.

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

The Student Management System Policy will include a section that will specify the completion of an internal audit checklist that will be completed with the review of the audit logs on a semi-annual

basis by November 30<sup>th</sup> and April 30<sup>th</sup> of each year. One of the items on the checklist will include a review of the bypassing of the lock out function.

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

The Student Management System Policy will include the requirement that all changes made to student grades be done so with a completed and signed Request for Grade Change Form. The form will specify the reason for the grade change and be signed by the Principal. Registrars will keep the forms on file in their office for 6 years.

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

This will be included in the internal audit checklist that will be developed with the Student Management System Policy.

We do believe that it is worth noting that according to the audit results, these users only made 4,809 grade changes out of 34,144 total grade changes or 14%. From a sample set of 90 of these grade changes, you only found that 5 of the 90 or about 5% of the grade changes were an increase or decrease grade change. The other 95% of the grade changes were the original entry of the grade by someone other than the teacher. We recognize the importance of having all of these grade entries and changes made by someone other than the teacher documented and will include this in the Student Management System Policy.

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

The workflow of the Request for Grade Change Form will include that a copy will be forwarded to Data Services after August 1st of each year to ensure that any changes are updated with the State Education Department (SED) to ensure that SED has the most current grade issued to a student on file.

- 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.*

The Student Management System Policy will require that access to the student grading system will be restricted based on title or role and that a staff member will receive the minimal access required to complete his/her job functions. This process is in place now. Review of user access rights will also be included in the internal audit checklist.

In reference to heightened permissions users, the 10 GST BOCES employees who have super user permissions provide direct support to the system and to the users. We agree that most of these users should not have grade modification permissions or assume-account permissions, however, we believe it is a current restriction of the system by the vendor to not have the ability to create a user with the ability to provide support but not have super user permissions. We will pursue a modification of the system with the vendor to allow this ability and increase the control we have over who has access to these heightened permissions. In the meantime, we will include the review of the usage of the assume-identity and the assume-account features in the internal audit checklist to ensure that their usage is consistent with the purpose of providing end-user technical support and not to make changes to data that should not be changed without the proper documentation.

- 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.*

The Student Management System Policy will specify that a user who needs additional permissions outside of the scope of his or her title or role will require the approval of the Director of Student Services and the Technology Director. This process is currently in writing via email, however, an electronic form system is under development to document the approval process in the near future.

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

This has already been done. The creation of the electronic form system should ensure that this process is tightened up.

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

We do believe that the assume-identity feature is appropriate for use for direct end-user support reasons. The assume-account feature is used much less frequently and should only be used in cases where technical support is required to troubleshoot a technical issue that is not resolved with the assume-identity feature. As previously noted, the use of these features will be included in the internal audit checklist to ensure that there is not inappropriate use of this feature.

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

We recognize the importance of the review of available audit logs and as previously noted, will be included in the Student Management System Policy. The work completed by the Comptroller's auditors provides us with an excellent starting point to develop an internal audit checklist that will be used to monitor the audit logs for unusual or inappropriate activity on a semi-annual basis.

- 11. The Board should adopt written policies and procedures for adding users, establishing users' access rights, deactivating or modifying user accounts, and monitoring user access.*

RE: Responses to Audit  
June 5, 2015  
Page 4

We anticipate being able to present the Student Management System Policy to the Board this summer for approval prior to the start of the 2015-2016 school year.

Thank you, once again, for your report and we look forward to addressing your recommendations. A detailed Corrective Action Plan is being developed and will be presented to the Board of Education for approval as required by law.

Sincerely,

Hillary J. Austin, Superintendent  
Elmira City School District

## **APPENDIX B**

### **AUDIT METHODOLOGY AND STANDARDS**

We reviewed access to the District's Student Grading System for the period July 1, 2013 through January 8, 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 GST BOCES 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.