OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY

Holland Patent Central School District

Access to the Student Information System

Report of Examination

Period Covered:

July 1, 2015 – July 31, 2016

2016M-326

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

January 2017

Dear School District Officials:

A top priority of the Office of the State Comptroller is to help school district officials manage their districts 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 districts' 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.

Following is a report of our audit of the Holland Patent Central School District, entitled Access to the Student Information System. 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 audit's results and recommendations are resources for district officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

Office of the State Comptroller
Division of Local Government
and School Accountability

Introduction

Background

The Holland Patent Central School District (District) is located in the Towns of Deerfield, Floyd, Marcy, Remsen, Steuben, Trenton and Western in Oneida County and the Town of Russia in Herkimer County. The District operates four schools with approximately 1,500 students and 300 employees. The District's budgeted appropriations for the 2015-16 fiscal year were approximately $31 million, which were funded primarily with State aid and real property taxes.

The District is governed by the Board of Education (Board), which is composed of five elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the District's chief executive officer and is responsible, along with other administrative staff, for the day-to-day management of the District under the Board's direction.

The District has established a technical team that is composed of the Superintendent, Superintendent of Buildings and Grounds, Assistant Superintendent for Business and Finance, Technology Coordinator and representatives from the Mohawk Regional Information Center (MORIC) and the Oneida-Herkimer-Madison Board of Cooperative Educational Services. The Assistant Superintendent for Curriculum and Instruction and the technical team, with support from other MORIC personnel, are responsible for the day-to-day operations of the student information system (SIS).

The SIS is an electronic system that serves as the official District record of student performance and is used to track students' grades (entered by District personnel), generate student report cards and maintain student permanent records (i.e., transcripts). The SIS also contains other personal, private and sensitive information (PPSI)[1] about students, including their student identification numbers and medical, order of protection and custody information.

Authorized SIS users are teachers, administrators, various other District employees, students' parents and third parties including MORIC employees and the SIS software vendor. Parents' access is limited to viewing (but not modifying or deleting) their children's student records and, therefore, we excluded those users from our audit

[1] PPSI is any information which – if subjected to unauthorized access, disclosure, modification, destruction or disruption of access or use – could severely affect critical functions, employees, customers (students), third parties or citizens of New York State in general.

testing. The District assigns access permissions to the 201 remaining (non-parent) users through 23 different user groups.[2]

Objective

The objective of our audit was to determine if District officials adequately safeguarded PPSI in the SIS. Our audit addressed the following related question:

- Did District officials adequately safeguard PPSI in the SIS?

Scope and Methodology

We examined the safeguarding of PPSI in the District's SIS for the period July 1, 2015 through July 31, 2016. Our audit also examined the adequacy of certain information technology controls. Because of the sensitivity of some of this information, we did not discuss certain audit results in this report but, instead, communicated them confidentially to District officials.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit are included in Appendix C of this report. Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

Comments of District Officials and Corrective Action

The results of our audit and recommendations have been discussed with District officials, and their comments, which appear in Appendix A, have been considered in preparing this report. Except as specified in Appendix A, District officials generally agreed with our recommendations and indicated they planned to take corrective action. Appendix B includes our comments on the issues raised in the District's response letter.

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of General Municipal Law, Section 2116-a (3)(c) of 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 provided to our office within 90 days, with a copy forwarded to the Commissioner of Education. 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.

[2] User groups are established in the SIS. All individuals in a group have the same user permissions.

Access to the Student Information System

Parents and students rely on District officials to ensure that students' PPSI is properly safeguarded. The Assistant Superintendent for Curriculum and Instruction and the technical team, with support from other MORIC personnel, are responsible for protecting and preventing improper access to this information. These individuals should ensure that users are not granted more permissions than necessary to perform their job duties and that SIS audit logs[3] are monitored for inappropriate activity. To guide these efforts, the technical team should ensure procedures are effective for managing and monitoring SIS access.

District officials granted unnecessary permissions for changing student grades, assuming accounts and identities,[4] and viewing PPSI. As a result, 17 users had permissions to change grades even though they were not responsible for doing so. Further, two users made 32 grade changes and permission forms could not be located for 13 of these grade changes. Also, 15 users (including 10 MORIC employees) could assume other SIS users' accounts and/or identities and one user (a MORIC employee) assumed six different SIS identities seven times. Further, two MORIC technicians who support the SIS servers but not the system itself can view the SIS audit log, which contains students' medical information, dates of birth and home addresses. Because the SIS does not generally create records in the audit log when users view information, we could not determine whether PPSI has been accessed inappropriately. These activities were not detected and investigated by officials because, at the times, officials did not routinely monitor audit logs. Stronger procedures would help officials safeguard PPSI from potential unauthorized activity that may not be detected and addressed in a timely manner.

Changing Grades

The District's grading policy establishes requirements for maintaining the official record of student grades. This record should be accurate and preserved to ensure its integrity as the historical record of student performance, credit accumulation, report cards and student transcripts. In addition, educators and the public evaluate school districts locally, regionally and nationally based on common student performance measures. To minimize the risk that grades could be changed inappropriately, permissions that allow for changing student grades should be restricted to those responsible for doing so.

---

[3] System-generated trails of user activities

[4] Assuming an identity allows a user to view (but not modify) SIS information. Assuming an account similarly allows a user to view information and perform any other activity that the assumed account can perform (for example, changing grades or modifying SIS permissions).

We examined SIS activity and high-risk SIS permissions[5] for the 201 users and found 17 users could change grades even though they were not responsible for doing so.

- One guidance office secretary made 31 changes to 10 students' grades and a second guidance office secretary made one change to a student's grade. Officials provided permission forms to justify and authorize 19 of the 32 grade changes but were unable to locate the remaining 13 permission forms. One of the 13 unsupported grade changes was a final course grade change from a 64 to a 65 (from a failing grade to a passing grade); the remaining unsupported changes were for marking period grades.

- One high school secretary, one pupil personnel services secretary, two county probation officers and a Sheriff's office resource officer had the ability to change grades.

- Ten MORIC employees had the ability to change certain types of grades. According to MORIC officials, the District does not record these types of grades in its SIS.

Permissions to change grades were granted to the seven users not employed by MORIC because all users involved in counseling activities were granted the same SIS permissions, even though some of these users required lesser permissions than others.

As a result of our audit, officials requested grade change permissions be removed for the two guidance office secretaries and the 10 MORIC employees. Officials also developed a plan to improve the grade change documentation and approval process. However, unless the ability to change grades in the SIS is restricted to those responsible for doing so, the risk will remain that student grades could be changed inappropriately or without authorization.

Assuming Accounts and Identities

The SIS allows users to assume other users' accounts and identities. Users with such account permissions do not need authorization from the account owner to assume his or her account or identity, and they do not need to enter that user's password. MORIC personnel indicated this functionality is necessary for troubleshooting and access management purposes. Because assuming an account or identity could allow individuals to view information or perform functions they could not within their own accounts, to prevent inappropriate activity, only individuals who have a job-related need for this function should be granted these permissions.

[5] High-risk SIS permissions allow granting or changing SIS access, assuming accounts or identities, viewing the SIS audit log, changing grades, or viewing students' identification numbers, medical information, order of protection information or custody information.

We found five users who could assume other users' accounts and identities without any job-related need to do so, including one high school secretary, one pupil personnel services secretary, two county probation officers and a Sheriff's office resource officer. The technical team requested that the assume account permissions be removed for these five users in June 2016, but MORIC personnel had not implemented this change as of the date of our testing nearly a month later, and officials were unaware that the requested change had not yet been made. They did not request the assume identity permission be removed at that time because similar users (also involved in counseling activities) needed that permission.

We also found 10 MORIC employees on the data analysis and verification team could assume other users' identities. One MORIC employee assumed six different SIS identities seven times between April and June 2016. Officials indicated this activity was appropriate given his support role, and we found no evidence that SIS information was added, modified or deleted using that account when the SIS identities were assumed.

While we found no inappropriate use, these powerful permissions should be strictly controlled and monitored to prevent inappropriate activity.

Viewing PPSI

The SIS contains PPSI including student identification numbers and students' medical, order of protection and custody information. The SIS audit log also contains PPSI including medical information, dates of birth and home addresses. District officials are responsible for preserving the confidentiality and integrity of this information. To prevent inappropriate access to PPSI, access to the SIS audit log should be restricted to those who need it to perform their job duties.

Two MORIC technicians who support the SIS servers but not the system itself can view the SIS audit log even though they do not need it to perform their job duties. Because the SIS does not generally create records in the audit log when users view information, we could not determine whether PPSI has been accessed inappropriately. Because officials would also be unable to use this log to detect unauthorized or inappropriate access to PPSI in the SIS, it is especially important to limit access to those who need to view this information to perform their job duties.

Managing Permissions and Monitoring

The Assistant Superintendent for Curriculum and Instruction and the technical team should ensure SIS activity is monitored for inappropriate activity. To guide these efforts, the technical team should ensure procedures are effective for managing and monitoring access. District officials should properly manage permissions so that

users have the least amount of access necessary to perform their job duties. Also, District officials should review the SIS audit logs to monitor for inappropriate activity.

As discussed in this report, District officials did not ensure permissions were properly assigned and maintained. These activities were not detected and investigated by officials because, at the times, officials did not routinely monitor audit logs.

Officials generally assigned SIS permissions to users according to their roles (e.g., teachers or counselors), but unique responsibilities were not always considered. As a result, some users were granted more permissions than needed, including the users who were unnecessarily able to change grades. The Assistant Superintendent for Curriculum and Instruction and the technical team indicated they annually review SIS accounts and permissions and request that MORIC personnel make any necessary changes. However, MORIC personnel do not always implement requested changes in a timely manner, and District officials do not perform follow up reviews to ensure all necessary changes have been made. Also, District and MORIC personnel indicated that, in July 2016, they began annual reviews of grade changes, attendance and activity related to assuming accounts and identities but, during our audit period, there was no process for reviewing SIS audit logs.

Because officials do not properly manage permissions or review the SIS audit logs to monitor for inappropriate activity, users are assigned more permissions than needed for their job duties and could use their access for questionable SIS activity. The unnecessary permissions may have been prevented or corrected had officials established stronger procedures. Therefore, it is especially important that officials ensure the newly established review process is effective in detecting questionable SIS activity such as that described in this report and in taking follow-up or remediation steps.

Recommendations

The Assistant Superintendent for Curriculum and Instruction and the technical team should work with other MORIC personnel to:

1. Evaluate permissions currently granted to each SIS user and remove any deemed unnecessary. Permissions that should be evaluated include those for the high school secretary, the pupil personnel services secretary, two county probation officers, the Sheriff's office resource officer and MORIC technicians.

2. Limit the ability to assume other SIS users' accounts and identities to those individuals that have a job-related need for this function and monitor for inappropriate activity.

The technical team should:

3. Review current procedures and strengthen controls to ensure that individuals have only those permissions needed to perform their job duties. This includes performing follow-up reviews with MORIC personnel to ensure they have made all necessary changes.

4. Ensure the newly established review process detects unauthorized or inappropriate SIS activity and allows officials to take follow-up or remediation steps in a timely manner.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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

The District's response letter refers to page numbers that appeared in the draft report. The page numbers have changed during the formatting of this report.

HOLLAND PATENT CENTRAL SCHOOL DISTRICT

9601 Main Street
Holland Patent, New York 13354

Kathleen M. Davis, Ed.D
Superintendent of Schools
(315) 865-7221

Cheryl Venettozzi, Ed.D
Assistant Superintendent
Business & Finance
(315) 865-7200

Nancy Nowicki
Assistant Superintendent
Curriculum & Instruction
(315) 865-7200

Mary Beth Piejko
Pupil Personnel &
CSE Chairperson
(315) 865-4148

High School
(315) 865-8154
Russell Stevener
Principal

Tamara Barbour
Athletic Director/
Assistant Principal
(315) 865-7273

HS Guidance Dept.
(315) 865-4102

Middle School
(315) 865-8152
Lisa Gentile
Principal

Michael Sinacore
Dean of Students

MS Guidance Dept.
(315) 865-7204

Gen. Wm. Floyd Elementary School
Kristin Casab
Principal
(315) 865-5721

Holland Patent Elementary School
James DeAngelo
Principal
(315) 865-8151

Dennis J. Geer
Superintendent of
Buildings & Grounds
(315) 865-7213

Christopher Roberts
Transportation Supervisor
(315) 865-4103

Rebecca Wilcox

Chief Examiner, Syracuse Regional Office

State Office Building, Room 409

New York Office of the State Comptroller

333 E. Washington Street

Syracuse, New York 13202-1428

RE: Comptroller's Audit Response

Dear Ms. Wilcox and Audit Team:

Thank you for your Report of Examination regarding the Access to the SIS for the Holland Patent Central School District. We found the audit to be helpful and informative to further assist the district in ensuring the safety guards for PPSI in SIS.

In response to the audit I present the following feedback in response to the audit conducted by your team:

Background Information: The Technical Team is inclusive of the Assistant Superintendent of Business and Finance. The Secretary to the District Superintendent was available during the audit but is not an active member of this committee.

See Note 1 Page 14

Access to Student Information:

The audit presents the following: "17 users had permissions to change the grades even though they were not responsible for doing so" (p. 6).

District Response:

As part of the support duties of 10 of the 17 users from the Regional Information System the district feels they could potentially need rights to student data as part of their current duties. The district met with the Regional Information Center on November 28, 2016 and requested that they be removed and activated as needed through administrative approvals from the district as well as the RIC.

Seven district employees are part of the PPS department and were placed in the guidance suite of SIS as their job descriptions and needs were aligned closest with this module. The district has worked with the vendor and the RIC to further modify their rights as noted in the audit.

We agree with the audit that these users have used the system appropriately and have not misused rights afforded to them.

The audit presents the following: "Two users made 32 grade changes and permissions could not be found for 13 of these changes" (p. 6).

District Response:

The two users who were identified in the audit are guidance secretaries who work under the direction of the principals and guidance counselors. The permission forms were an internal process that the district implemented in October 2015. The team has been retrained on the form as well as the Assistant Superintendent for Curriculum and Instruction verified that all changes were appropriate. The guidance secretaries' rights have been modified.

The audit presents the following: "Two technicians who support services but not the system itself can view SIS logs."

District Response:

The district met with the RIC leadership team to confirm that the two technicians do in fact support the servers. The system does not allow for this component to be restricted from their rights without deleting from them from the components they need. It should be noted that they have been trained in proper handling of PPSI and have appropriately navigated the system.

The audit presents the following: "Officials did not routinely monitor audit logs"

District Response:

The district does have documented procedures to monitor audit logs twice a year. This process has been utilized. The district will continue to meet regarding the logs and will look more specifically at creating new groups within the modules to offer a more precise scope for users.

See Note 2 Page 14

The audit presents the following: "Because Officials do not properly manage permission or review the SIS audit logs to monitor for inappropriate activity users are assigned more permissions:

District Response:

The Holland Patent Central Schools District does have a documented procedure for reviewing audit logs two times per year (December/ June). The program has set user groups as part of the software design. The vendor, RIC and the District will continue to work together to modify the software to accommodate our needs.

See Note 2 Page 14

The audit presents the following: "Officials provided permission forms to justify and authorize 19 of the 32 grade changes but were unable to locate 13 permission forms."

District Response:

The Assistant Superintendent has verified that all 13 changes were appropriate. The internal grade change form needs to be used consistently. This form has been reviewed with staff and rights for key staff have been modified to limit users.

The audit presents the following: "15 users could assume SIS user accounts or identities" (p. 7).

District Response:

As aforementioned, 15 users were assigned initially to the "guidance group" of SIS. All 15 users applied their rights appropriately as noted by this audit. Holland Patent CSD has modified user accounts with the RIC and the vendor to limit access as required by job tasks.

Audit Summary:

The Holland Patent CSD is extremely pleased with audit findings that all users with access to the SIS system were using the tool appropriately. The district has made the necessary modifications to user rights and have provided further guidance on the use of the district internal process for grade changes.

We appreciate the time and expertise of the audit team as they provided a great deal of support and information for district consideration.

Sincerely,

Dr. Kathleen M. Davis

Superintendent

Dr. Cheryl Venettozzi

Assistant Superintendent for Business and Finance

C: Log Audit File

Board of Education

APPENDIX B

OSC COMMENTS ON THE DISTRICT'S RESPONSE

Note 1

We modified our report to update the members of the technical team.

Note 2

As noted in our report, District and MORIC personnel indicated that, in July 2016, they began annual reviews of grade changes, attendance and activity related to assuming accounts and identities but, during our audit period, there was no process for reviewing SIS audit logs.

APPENDIX C

AUDIT METHODOLOGY AND STANDARDS

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

- We interviewed District and MORIC personnel to gain an understanding of the SIS and related information technology controls.

- We compared all SIS users' job roles with user group assignments to determine if high-risk permissions are compatible with responsibilities. For all users with questionable access, we interviewed District officials to determine if users had responsibilities that required the permissions in question.

- We analyzed SIS audit logs for indications of unauthorized access or inappropriate use.

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.

APPENDIX D

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller
Public Information Office
110 State Street, 15th Floor
Albany, New York 12236
(518) 474-4015
http://www.osc.state.ny.us/localgov/

APPENDIX E

OFFICE OF THE STATE COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY

Andrew A. SanFilippo, Executive Deputy Comptroller
Gabriel F. Deyo, Deputy Comptroller
Tracey Hitchen Boyd, Assistant Comptroller

LOCAL REGIONAL OFFICE LISTING

BINGHAMTON REGIONAL OFFICE
H. Todd Eames, Chief Examiner
Office of the State Comptroller
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313
Email: Muni-Binghamton@osc.state.ny.us

Serving: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins Counties

BUFFALO REGIONAL OFFICE
Jeffrey D. Mazula, Chief Examiner
Office of the State Comptroller
295 Main Street, Suite 1032
Buffalo, New York 14203-2510
(716) 847-3647 Fax (716) 847-3643
Email: Muni-Buffalo@osc.state.ny.us

Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming Counties

GLENS FALLS REGIONAL OFFICE
Jeffrey P. Leonard, Chief Examiner
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, New York 12801-4396
(518) 793-0057 Fax (518) 793-5797
Email: Muni-GlensFalls@osc.state.ny.us

Serving: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington Counties

HAUPPAUGE REGIONAL OFFICE
Ira McCracken, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788-5533
(631) 952-6534 Fax (631) 952-6530
Email: Muni-Hauppauge@osc.state.ny.us

Serving: Nassau and Suffolk Counties

NEWBURGH REGIONAL OFFICE
Tenneh Blamah, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725
(845) 567-0858 Fax (845) 567-0080
Email: Muni-Newburgh@osc.state.ny.us

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester Counties

ROCHESTER REGIONAL OFFICE
Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street, Suite 522
Rochester, New York 14614-1608
(585) 454-2460 Fax (585) 454-3545
Email: Muni-Rochester@osc.state.ny.us

Serving: Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates Counties

SYRACUSE REGIONAL OFFICE
Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428
(315) 428-4192 Fax (315) 426-2119
Email: Muni-Syracuse@osc.state.ny.us

Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence Counties

STATEWIDE AUDITS
Ann C. Singer, Chief Examiner
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313