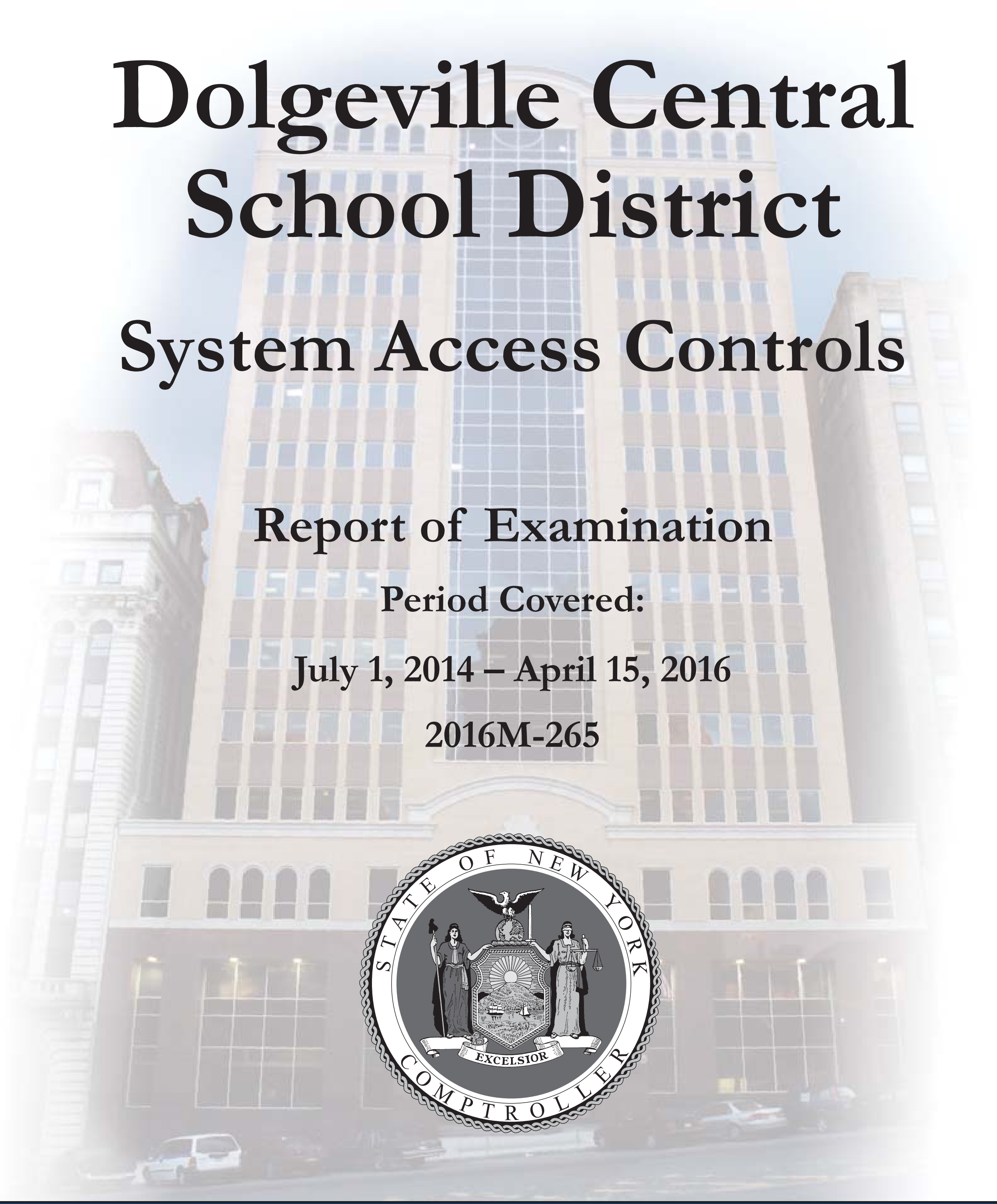
OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY



Dolgeville Central School District

System Access Controls

Report of Examination

Period Covered:

July 1, 2014 – April 15, 2016

2016M-265

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 Dolgeville Central School District, entitled System Access Controls. 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 Dolgeville Central School District (District) is located in the Towns of Fairfield, Manheim and Salisbury in Herkimer County and the Towns of Ephratah, Oppenheim and Stratford in Fulton County. The District is governed by the Board of Education (Board), which is composed of seven 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 District's day-to-day management under the Board's direction. The Business Administrator, with support from the technology coordinator, is responsible for the day-to-day operations of the financial system (FS). The high school guidance counselor, with support from the technology coordinator and the Mohawk Regional Information Center (MORIC), is responsible for the day-to-day operations of the student information system (SIS).

The District operates three schools with 918 students and 185 employees. The District's budgeted appropriations for the 2015-16 fiscal year were approximately $19 million, funded primarily with State aid and real property taxes.

The FS is an electronic system used to record employee and vendor information (entered by District personnel); generate, sign and print checks; and post journal entries to the general ledger. The FS contains personal, private and sensitive information (PPSI)[1] about District employees, including their Social Security numbers and bank, retirement and health savings account information. Authorized FS users are the Business Administrator, Deputy Treasurer, Treasurer, Clerk and Business Office secretary. The District assigns access permissions to these users within five different software modules.

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

[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, third parties or citizens of New York State in general.

information. Authorized SIS users are teachers, administrators, various other District employees and third parties, including MORIC employees and the SIS software vendor. The District assigns access permissions to these 186 users through 18 different user groups.[2]

Objective

The objective of our audit was to examine information technology (IT) access controls over PPSI in the District's FS and SIS. Our audit addressed the following related question:

- Did District officials implement IT access controls to adequately safeguard PPSI in the District's FS and SIS?

Scope and Methodology

We examined the District's IT access controls for the period July 1, 2014 through April 15, 2016. 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 B 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. District officials generally agreed with our recommendations and indicated they planned to take corrective action.

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 and permissions are assigned by group. Therefore, all individuals in a group have the same user permissions.

System Access Controls

Employees and students rely on District officials to ensure that their PPSI is properly safeguarded. The Business Administrator and high school guidance counselor, with support from the technology coordinator and MORIC personnel, are responsible for protecting and preventing improper access to this information. To fulfill these responsibilities, the Business Administrator and high school guidance counselor should ensure that FS and SIS user accounts for District and third-party personnel are removed when access is no longer needed, users are not granted more permissions than necessary to perform their job duties and audit logs[3] are monitored for indications of inappropriate activity. To guide these efforts, officials should develop comprehensive written procedures for managing FS and SIS access and reviewing audit logs.

District officials have not implemented adequate IT access controls for safeguarding PPSI in the FS and SIS. We found unnecessary FS and SIS user accounts, including a built-in FS account that was not removed and other accounts for former employees, former long-term substitutes and current employees who do not need access. We also found questionable FS access and suspicious access attempts that were not detected and investigated by officials. In addition, we found unnecessary FS permissions for creating employee records and viewing employees' PPSI and unnecessary SIS permissions for changing student grades, assuming SIS identities and viewing students' PPSI. Unnecessary accounts and permissions increase the risk of unauthorized access and potentially harmful modification, use or exposure of PPSI.

While we found no evidence of abuse of these accounts and permissions, our ability to review FS and SIS activity is limited due to deficiencies in the systems' audit logging capabilities. However, officials did not effectively use all information available in the audit logs to properly monitor FS and SIS use. This essential control would help to safeguard PPSI from potential unauthorized activity that may not be detected and addressed in a timely manner.

User Accounts

To minimize the risk of unauthorized access, FS and SIS user accounts should be limited to those individuals who currently need access to one or more functions to perform their job duties. Access should be terminated promptly when employees leave the District or no longer need access to perform their job duties. Such controls limit the risk that PPSI will be exposed to unauthorized use or modification.

[3] System-generated trails of user activities

We found that three of the eight FS user accounts between July 1, 2014 and April 12, 2016 (38 percent) and 20 of the 186 SIS user accounts as of April 15, 2016 (11 percent) were unnecessary.

- The three unnecessary FS accounts include a built-in user account that has not been removed, an existing account for a former employee and a recently removed account for another former employee (this account was removed nearly two years after the employee left the District). The built-in user account was used nine times from three different District computers during our audit period. Neither of the other two unnecessary accounts were used after the employees left the District.

- The 20 unnecessary SIS accounts were created for 10 former employees, six former long-term substitutes and four current employees who do not need SIS access. We found no evidence that SIS information was added, modified or deleted using the 10 accounts for former employees after those employees left the District. We also found no evidence that the remaining 10 unnecessary accounts were used inappropriately.

These unnecessary accounts were not identified and corrected because, while officials have established policies regarding the confidentiality of employee and student PPSI, they have not developed written procedures to support compliance with these policies, including those for reviewing user access to this information. As a result, FS and SIS user accounts were not reviewed and removed timely.

Unnecessary accounts are potential entry points for attackers as they could be used to inappropriately access and view PPSI in the FS or the SIS. Further, unnecessary accounts create additional work to manage permissions along with the risk of errors that could result in users being inadvertently granted more access than needed.

Activity and Permissions

The FS contains PPSI about employees including their Social Security numbers and bank, retirement and health savings account information. The FS also contains information critical for determining the District's financial condition. Similarly, the SIS contains PPSI, including student identification numbers and students' medical, order of protection and custody information, and information critical for recording student performance. Officials should preserve the confidentiality and integrity of this information by restricting FS and SIS permissions to those necessary for users to perform their job duties. The Business Administrator should also grant FS access in a manner that prevents users from being involved in multiple aspects of financial transactions and implement compensating controls, such as increased oversight, wherever segregation is impractical.

We examined FS activity during our audit period as well as the high-risk FS permissions[4] for the system's five necessary users. We found the following:

- The unnecessary built-in account was used to log into the various FS modules nine times from three different computers. We also found two invalid password attempts associated with this account from one computer. Officials cannot be sure who is responsible for the activity using this account because it is used by more than one user and accounts are commonly accessed from multiple computers.

- During a one-hour time period, 12 invalid passwords were entered for a FS account. Because officials do not regularly review the audit log, they were not aware of the suspicious activity and did not take the appropriate follow-up steps to ensure the account had not been compromised. We followed up at the time of our testing and the user indicated that this was not an unauthorized access attempt.

- Incompatible duties have not been segregated as both the Deputy Treasurer and Treasurer have access to all available FS functions except administering the system. This issue was identified during a third-party risk assessment in 2007 and our previous audit in 2008. However, implemented compensating controls (namely, the Business Administrator's review and approval of all purchase orders and journal entries) would not prevent the granted permissions from being used to conduct inappropriate activity nor enable officials to detect abuse of the permissions. Officials should consider additional compensating controls such as periodic reviews of FS information including employees and their salaries.

- The Business Office secretary unnecessarily has permissions to create employee records in the FS and to view employees' Social Security numbers and their retirement, insurance and salary information. These unnecessary permissions were granted because the Business Administrator grants users all permissions within the modules they need to access rather than limiting access to necessary permissions within those modules.

[4] We defined high-risk FS permissions as those that allow viewing PPSI or adding, modifying or deleting critical information in the system.

We also examined SIS activity during our audit period as well as the high-risk SIS permissions[5] for the system's 186 users. We found the following:

- The SIS had 10 users who improperly had permissions to change grades when they did not have the responsibility to do so. While we did not identify any grade changes made in the SIS by these users, the risk exists that student grades could be changed inappropriately or without authorizations.

- A MORIC employee on the data analysis and verification team who, according to MORIC officials, should not be able to assume SIS identities[6] did so five times. Officials indicated that this activity was necessary and related to her job and we found no evidence that SIS information was added, modified or deleted using that account during our audit period. A teacher assistant and eight additional MORIC employees also had unnecessary permissions to assume identities but did not do so during our audit period.

- A Business Office secretary was unnecessarily able to view students' medical information and two MORIC technicians, who support the SIS servers but not the system itself, were unnecessarily able to view the SIS audit log, which contains medical information, dates of birth and home addresses. Because the SIS does not generally record when users view information, we could not determine whether these permissions were used inappropriately.

Questionable activities were not identified and investigated because officials do not regularly review FS or SIS audit logs. Because we found that users are assigned more permissions than needed for their job duties, it is especially important that District officials monitor user activities to help detect inappropriate FS and SIS use. However, we found that the FS audit logs do not generally record when users view, enter, modify or delete information in the system and that, while the SIS audit log does record when users enter, modify or delete information, it does not generally record when users view information.

[5] We defined high-risk SIS permissions as those that allow managing user accounts; 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.

[6] Assuming an identity allows a user to view (but not modify) information in the SIS for students assigned to the assumed identity/user. The SIS further allows users to assume accounts, which similarly allows them to view student information, and also to perform any other activity the assumed accounts have permissions to perform (for example, changing grades or modifying SIS permissions).

Therefore, because officials would be unable to use the logs to detect certain unauthorized or inappropriate activities, minimizing FS and SIS access is especially critical.

Unnecessary permissions were not prevented or corrected because officials have not established effective procedures for assigning FS and SIS permissions. Further, while the technology coordinator and MORIC personnel are, to an extent, involved in managing FS and SIS access, the District has assigned primary responsibility to the Business Administrator and the high school guidance counselor, respectively. These individuals should be provided the training and technical knowledge necessary to minimize the risk of unintentional errors or misunderstandings in granted access.

Recommendations

The Business Administrator (with respect to the FS) and the high school guidance counselor (with respect to the SIS), with support from the technology coordinator and MORIC personnel as needed, should:

1. Evaluate all existing FS and SIS user accounts and remove any account deemed unnecessary.

2. Establish written procedures for managing and monitoring FS and SIS access. These procedures should include guidance for assigning permissions and monitoring user access.

3. Determine whether use of the built-in FS account is appropriate or if access to the FS should be limited to unique user accounts.

4. Ensure FS and SIS audit logs are periodically reviewed for indications of unauthorized or inappropriate activity.

5. Evaluate permissions currently granted to each FS and SIS user and remove any permission deemed unnecessary or incompatible.

6. Review current procedures for assigning and monitoring FS and SIS permissions and strengthen controls to ensure that individuals are assigned only those permissions needed to perform their job duties.

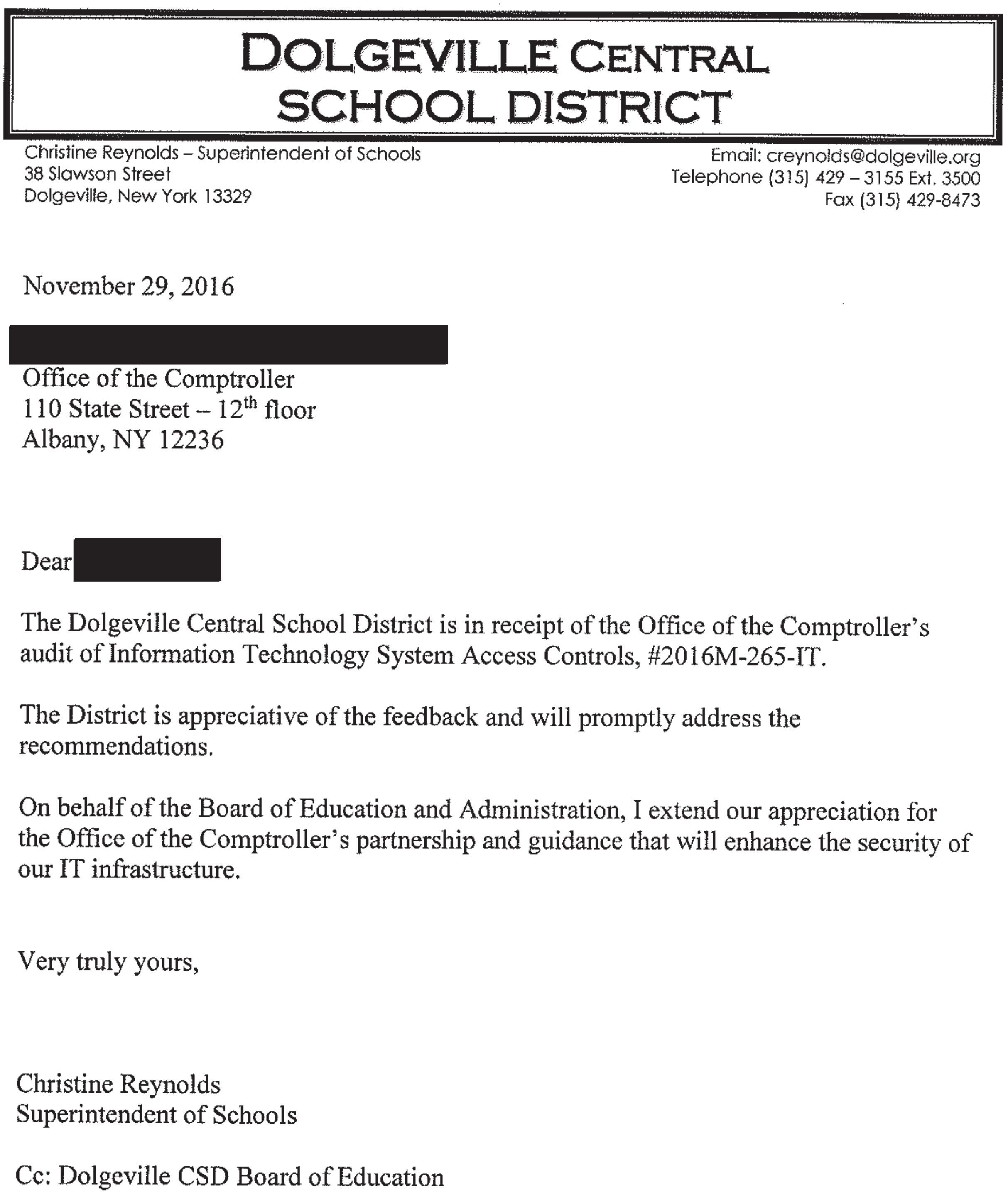
The Superintendent should:

7. Ensure that individuals assigned responsibility for managing FS and SIS accounts and permissions are provided the training and technical knowledge necessary to minimize the risk of unintentional errors or misunderstandings in granted access.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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



DOLGEVILLE CENTRAL SCHOOL DISTRICT

Christine Reynolds – Superintendent of Schools
38 Slawson Street
Dolgeville, New York 13329

Email: creynolds@dolgeville.org
Telephone (315) 429 – 3155 Ext. 3500
Fax (315) 429-8473

November 29, 2016

[redacted]
Office of the Comptroller
110 State Street – 12th floor
Albany, NY 12236

Dear [redacted]

The Dolgeville Central School District is in receipt of the Office of the Comptroller's audit of Information Technology System Access Controls, #2016M-265-IT.

The District is appreciative of the feedback and will promptly address the recommendations.

On behalf of the Board of Education and Administration, I extend our appreciation for the Office of the Comptroller's partnership and guidance that will enhance the security of our IT infrastructure.

Very truly yours,

Christine Reynolds
Superintendent of Schools

Cc: Dolgeville CSD Board of Education

APPENDIX B

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 District's FS, SIS and related IT access controls.

- We compared a list of active District employees to lists of current FS and SIS users to determine if any FS or SIS users were not District employees or if any former employees remained on the user lists. For all users that are not current or former District employees, we interviewed District and MORIC personnel to determine if those users provide technology or other support that requires access to the FS or SIS.

- We compared all FS and SIS users' job roles with reports of users' permissions and user group assignments, respectively, to determine if high-risk permissions are compatible with responsibilities. For all users with questionable access, we interviewed District officials to determine if users have responsibilities that require the permissions in question.

- We analyzed the audit logs generated by the FS and SIS 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 C

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 D

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