Office of the New York State Comptroller

Division of Local Government
& School Accountability

West Canada Valley Central School District

Access to the Student Information System

Report of Examination

Period Covered:

July 1, 2014 – January 31, 2016

2016M-96

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

July 2016

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 West Canada Valley 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 West Canada Valley Central School District (District) is located in the Towns of Fairfield, Herkimer, Manheim, Newport, Norway and Schuyler in Herkimer County and the Town of Deerfield in Oneida County. The District operates two schools with 679 students and 143 employees. The District's budgeted appropriations for the 2015-16 fiscal year are approximately $16 million, funded primarily with State aid and real property taxes.

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 day-to-day management of the District under the Board's direction. The Superintendent, with support from the Mohawk Regional Information Center (MORIC), is also 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 users of the SIS 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 142 users through 23 different user groups.[2]

Objective

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

- Did District officials implement IT access controls to adequately safeguard PPSI in its SIS?

[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.

[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.

Scope and Methodology

We examined the District's IT access controls for the period July 1, 2014 through January 31, 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.

Access to the Student Information System

Parents and students rely on District officials to ensure that students' PPSI is properly safeguarded. The Superintendent, with support from other District and MORIC employees, is responsible for protecting and preventing improper access to this information. To fulfill these responsibilities, the Superintendent should ensure that users are not granted more permissions than necessary to perform their job duties, user accounts for District and third-party personnel are removed when SIS access is no longer needed, and audit logs are monitored for indications of inappropriate activity. To guide these efforts, the Board should develop comprehensive written policies and procedures for managing SIS accounts and permissions and reviewing SIS audit logs.

We found unnecessary permissions granted for changing student grades, assuming accounts and identities, and viewing PPSI. For example, 29 users were able to change grades without having the responsibility and 11 users could assume other SIS users' identities without any job-related need to do so. Although these users did not actually change grades or assume other users' identities, the unnecessary ability to do so weakens controls over system integrity. We also found unnecessary SIS user accounts, including those for three former District employees.

During our audit period, SIS accounts were assumed approximately 140 times and SIS identities nearly 400 times by various users. None of this use was found to be inappropriate; however, unnecessary permissions and accounts increase the risk of unauthorized access and potentially harmful modification, use or exposure of PPSI. Due to the lack of effective management, permissions and accounts were not properly assigned or maintained in accordance with employees' job responsibilities and changing employment status. Further, officials did not properly monitor SIS use. This essential control would help to safeguard the District's PPSI from potential unauthorized activity that may not be detected and addressed in a timely manner.

Permissions

We examined high-risk SIS permissions[3] for the system's 142 users as of December 22, 2015 and identified the following unnecessary permissions that were granted:

- Twenty-nine users without the responsibility to change grades had permission to do so in the SIS.

[3] 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.

- One user had permissions to assume accounts and identities[4] unnecessarily and another 10 users had permission to assume identities unnecessarily.

- One user is unnecessarily able to view students' identification numbers, medical information, order-of-protection information, custody information and the SIS audit log. Two additional users are also unnecessarily able to view the SIS audit log.

Changing Grades – The District has a Student Grading Information Systems policy that establishes requirements for maintaining the official record of student grades. This record should be accurate and preserved to ensure its integrity as it serves 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.

Twenty-nine users without grade change responsibilities had been granted permission to change certain grades in the SIS: nine MORIC employees, seven teacher assistants, six study hall monitors, two account clerks, a teacher aide, a speech therapist, a school psychologist, a cafeteria manager and a transportation supervisor. These unnecessary permissions were granted because the Superintendent was not aware of all available SIS permissions. As a result, there is an increased risk that student grades could be changed inappropriately or without authorization.

Assuming Accounts and Identities – The SIS allows users to assume the account or identity of another user. MORIC personnel indicated that this functionality is necessary for troubleshooting and access management purposes. 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. Assuming an account or identity could allow individuals to view information or perform functions they could not perform within their own account. Therefore, to prevent inappropriate activity, only individuals who need this function to perform their job duties should be granted these permissions.

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

Between July 1, 2014 and January 26, 2016, SIS accounts were assumed approximately 140 times and SIS identities were assumed nearly 400 times. Users who assumed an account or identity include the Superintendent, the guidance and technology coordinators, the current and previous data coordinators, the previous Interim Superintendent/Principal, two secretaries, 15 MORIC employees (one who no longer works for the MORIC) and the SIS software vendor.

While none of this use was found to be inappropriate, we found that a teacher assistant had permissions to assume accounts and identities unnecessarily and another 10 users (nine MORIC employees and a school psychologist) had permissions to assume identities unnecessarily. These powerful permissions should be strictly controlled and monitored to prevent inappropriate activity by users who would not otherwise be able to perform those activities.

Viewing PPSI – The SIS contains PPSI including student identification numbers and medical, order-of-protection and custody information. The SIS audit log (a system-generated trail of user activities) also contains several PPSI items including medical information, home addresses and dates of birth. District officials are responsible for preserving the confidentiality and integrity of this information. To prevent inappropriate access to PPSI, the ability to view this information should be restricted to those who need it to perform their job duties.

We found one user, a teacher assistant, unnecessarily able to view students' identification numbers, medical information, order-of-protection information, custody information and the SIS audit log. We also found two additional users (both MORIC employees) unnecessarily able to view the SIS audit log. To safeguard against inappropriate disclosure or misuse, access to students' PPSI should be limited to those who need access to fulfill their job duties.

User Accounts

To minimize the risk of unauthorized access, SIS user accounts should be limited to those individuals who currently need access to one or more SIS 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.

We examined all 142 SIS user accounts as of December 22, 2015. Of these, eight had never been used to log into the SIS and an additional 23 had not been used to log in during the current school year. According to District and MORIC personnel, all but one of the accounts not used during the current school year are needed by current District or MORIC employees. The one unnecessary account is for the previous

data coordinator, who is now retired. We identified another three user accounts that were created for a teacher's aide who has no need to access the SIS, and two former study hall monitors (one who is still employed by the District but in another role that does not require SIS access). These four accounts have the ability to perform a variety of functions in the SIS, including viewing student PPSI. One of these accounts also has the ability to change certain student grades and assume SIS identities.

While we did not find any indication of inappropriate use, the risk exists that an unnecessary account could be used to inappropriately access the SIS. Further, unnecessary user accounts create additional work to manage SIS permissions, along with the risk of error, which could be avoided by reviewing and disabling or correcting these accounts as appropriate.

Management and Monitoring

The Superintendent should ensure that the SIS is monitored for unnecessary access or indications of inappropriate activity. To guide these efforts, the Board should develop comprehensive written policies and procedures for managing SIS accounts and permissions and reviewing SIS audit logs.

District officials do not sufficiently manage SIS accounts and permissions or review the SIS audit logs on a regular basis. In addition, they have not established effective policies and procedures for protecting PPSI in the SIS. The unnecessary permissions and accounts we identified may have been prevented or corrected had District officials sufficiently managed and monitored access.

Managing Accounts and Permissions – District officials should properly manage accounts and permissions to ensure access to the SIS is limited to those with a business need and users have the least amount of access necessary to perform their job duties. The Superintendent is responsible for coordinating with other District and MORIC employees to add and remove SIS accounts and permissions. According to District personnel, network user accounts are reviewed twice a year. However, the review process is informal, does not include retaining documentation, and would not identify unnecessary SIS permissions or all unnecessary SIS accounts. The Superintendent also indicated he is unsure of the meaning of the groups and permissions available and assigned in the SIS. These weaknesses resulted in the unnecessary permissions and accounts.

Reviewing Audit Logs – Audit logs maintain an automated record of activity in a computer application. District officials should review these logs to monitor for indications of inappropriate activity. However, they have not established a process for reviewing audit

logs on a regular basis. 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 use of the SIS. While we did not find any indication of inappropriate use of the granted permissions, without activity reviews District officials would be unaware of any inappropriate use and thus could not take appropriate follow-up or remediation steps.

Establishing Policies and Procedures – The District should have comprehensive written policies and procedures for protecting PPSI in the SIS. However, District officials have not established procedures for assigning permissions and monitoring SIS activity. While the Board adopted a Student Grading Information Systems policy for controlling access to the SIS in December 2015, not all District employees are aware of and following this policy. Finally, procedures for reviewing network user accounts are informal and ineffective for monitoring SIS accounts and permissions. Without proper policies and procedures, District and MORIC personnel may not understand their roles and responsibilities, or District officials' expectations, for granting and restricting SIS access.

Recommendations

The Superintendent, with support from MORIC personnel as needed, should:

1. Establish written procedures for adding users to the SIS, assigning permissions, modifying permissions, removing users and monitoring user activity.

2. Communicate the Student Grading Information Systems policy to all District employees and provide training as needed to clarify roles and responsibilities.

3. Evaluate permissions currently granted to each SIS user, including MORIC employees, and remove any permissions deemed unnecessary.

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

5. Strictly limit the ability to assume accounts and identities to designated individuals and monitor activity associated with these functions.

6. Evaluate all existing SIS user accounts and remove any accounts deemed unnecessary.

7. Work with the software vendor to gain a better understanding of the available SIS permissions and thoroughly test the permissions currently assigned to SIS users.

8. Ensure SIS audit logs are periodically reviewed for unauthorized or inappropriate activity.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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

West Canada Valley Central School District

5447 State Route 28 • P.O. Box 360
Newport, N.Y. 13416-0360
Telephone: 315-845-6800
Junior/Senior High School Fax: 845-8652
Elementary School Fax: 845-1640
Garage Fax: 845-8653
www.westcanada.org

Donald J. Sheparoson
Superintendent of Schools

John McKeown
Business Administrator

Correne M. Holmes
Elementary School
Principal

Frank C. Sutliff
Junior/Senior High School
Principal

Melissa M. Tubia
Guidance Coordinator

Felix W. Ray Jr.
Transportation Supervisor

Kenneth A. Smith
Director of Facilities

April 25, 2016

Rebecca Wilcox, Chief Examiner
333 East Washington Street
Syracuse, NY 13202

Dear Chief Examiner Wilcox:

RE: CORRECTIVE ACTION PLAN
Unit Name: West Canada Valley Central School District
Audit Report Title: Access to the Student Information System
Audit Report Number: 2016M-96

Recommendation

1. Establish written procedures for adding users to the SIS, assigning permissions, modifying permissions, removing users and monitoring user activity.

   Actions
   The District has reviewed current procedures for assigning user access rights and has strengthened controls to ensure that individuals are assigned only to rights needed to perform job duties and functions. Duties regularly change for employees depending on instructional and support assignments. Therefore, additional assurances including improved documentation of initial access, documentation to support adjustments to access, and documentation when access should be discontinued due to retirement or resignation have been initiated.

Recommendation

2. Communicate the Student Grading Information Systems policy to all District employees and provide training as needed to clarify roles and responsibilities.

   Actions
   The district subscribes to the BOCES Policy Service as a primary support for ensuring policies and procedures for school governance effectively support

Committed to preparing responsible, caring and productive citizens.

West Canada Valley Central School District

5447 State Route 28 • P.O. Box 360
Newport, N.Y. 13416-0360
Telephone: 315-845-6800
Junior/Senior High School Fax: 845-8652
Elementary School Fax: 845-1640
Garage Fax: 845-8653
www.westcanada.org

Donald J. Shepardson
Superintendent of Schools

John McKeown
Business Administrator

Correne M. Holmes
Elementary School
Principal

Frank C. Sutliff
Junior/Senior High School
Principal

Melissa M. Tubia
Guidance Coordinator

Felix W. Ray Jr.
Transportation Supervisor

Kenneth A. Smith
Director of Facilities

and safeguard district operations. Policies will be reviewed with key stakeholders and ongoing training will continue to clarify roles and responsibilities.

Recommendation

3. Evaluate permissions currently granted to each SIS user, including MORIC employees and remove any permission deemed unnecessary.

Actions

The District is working with the MORIC to identify the pathway of rights granted to each user group. As permissions are evaluated, eliminating the access to additional or unnecessary rights to any user will be corrected.

Recommendation

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

Actions

The District is working with the MORIC to identify the procedure for rights granted to each user group. As permissions are evaluated, eliminating the access to additional or unnecessary rights to any user will be remedied. Additionally, the user rights to individuals and groups have been clarified with the MORIC and monitoring has initiated.

Recommendation

5. Strictly limit the ability to assume accounts and identities to designated individuals and monitor activity associated with these functions.

West Canada Valley Central School District

5447 State Route 28 • P.O. Box 36
Newport, N.Y. 13416-036
Telephone: 315-845-680
Junior/Senior High School Fax: 845-865
Elementary School Fax: 845-164
Garage Fax: 845-865
www.westcanada.or

Donald J. Shepardson
Superintendent of Schools

John McKeown
Business Administrator

Correne M. Holmes
Elementary School
Principal

Frank C. Sutliff
Junior/Senior High School
Principal

Melissa M. Tubia
Guidance Coordinator

Felix W. Ray Jr.
Transportation Supervisor

Kenneth A. Smith
Director of Facilities

Actions

The District has limited the *assume* functions to designated officials. The District is working with MORIC to review the audit log report. This will allow to accurately identify user activity in the *assume* setting.

Recommendation

6. Evaluate all existing SIS user accounts and remove any accounts deemed unnecessary.

Actions

The District has removed unknown accounts that had once been created for ease of functioning and off-campus support. Staff members who require SIS access have been given direct access specific to their needs.

Recommendation

7. Work with the software vendor to gain a better understanding of the available SIS permissions and thoroughly test the permissions currently assigned to SIS users.

Action

The district will work with MORIC to develop groups that align with required permissions to perform assigned job duties. In addition, MORIC will thoroughly test these permissions to ensure staff are assigned to needed areas.

Recommendation

8. Ensure SIS audit logs are periodically reviewed for unauthorized or inappropriate activity.

West Canada Valley Central School District

5447 State Route 28 • P.O. Box 360
Newport, N.Y. 13416-0360
Telephone: 315-845-6800
Junior/Senior High School Fax: 845-8652
Elementary School Fax: 845-1640
Garage Fax: 845-8653
www.westcanada.org

Donald J. Shepardson
Superintendent of Schools

John McKeown
Business Administrator

Correne M. Holmes
Elementary School
Principal

Frank C. Sutliff
Junior/Senior High School
Principal

Melissa M. Tubia
Guidance Coordinator

Felix W. Ray Jr.
Transportation Supervisor

Kenneth A. Smith
Director of Facilities

Actions

The District will work with the MORIC to access and review audit logs to help identify unusual or inappropriate activity and increase checks and balances.

Conclusions

The full audit report has been shared with the Mohawk Regional Information Center along with the Technology Director. A collaborative effort has begun to address potential vulnerabilities under our current system.

Best practices to limit vulnerabilities to SIS including consistent review of audit-logs, permissions, and ongoing training for all West Canada Valley staff will only enhance the security of our current system. This will allow the Mohawk Regional Information Center to continue their support of the district as a valued resource to enhance student learning.

Signed:

D.J. Shepardson 6/10/16
Superintendent

Committed to preparing responsible, caring and productive citizens.

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 SIS and related IT access controls.

- We compared a list of active District employees to a list of current SIS users to determine if any SIS users are not District employees or if any former employees remained on the user list. 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 SIS.

- For all users with last login dates prior to the start of the current school year, we interviewed District officials to determine if those users have a current, legitimate business need to access the SIS.

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

- We analyzed the audit logs generated by the District's 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