DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2021M-22

# Whitesville Central School District

## Information Technology

JUNE 2021

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller

# Contents

**Report Highlights . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1**

**Information Technology . . . . . . . . . . . . . . . . . . . . . . . . . . 2**

Why Should the District Secure Access to the Network and Information Systems? . . . . . . . . . . . . . . . . . . . . . . . . . . . 2

Officials Did Not Adequately Secure User Accounts and Permissions 3

What Do We Recommend? . . . . . . . . . . . . . . . . . . . . . . . . 4

**Appendix A – Response From District Officials . . . . . . . . . . . . 5**

**Appendix B – Audit Methodology and Standards . . . . . . . . . . . 7**

**Appendix C – Resources and Services . . . . . . . . . . . . . . . . . . 9**

# Report Highlights

## Whitesville Central School District

## Audit Objective

Determine whether Whitesville Central School District (District) officials adequately secured access to the network and information systems.

## Key Findings

District officials did not adequately secure access to the network and information systems. District officials did not:

- Disable six unnecessary user accounts.
- Establish written policies or procedures to monitor shared accounts or for adding, modifying or disabling user permissions to the network and information systems.
- Establish a written agreement with the Erie 1 Board of Cooperative Educational Services (BOCES) to define information technology services to be provided.

In addition, sensitive IT control weaknesses were communicated confidentially to officials.

## Key Recommendations

- Disable unnecessary accounts.
- Adopt a written user permissions policy and establish written procedures for adding, modifying and disabling user permissions and for monitoring shared accounts.

District officials agreed with our recommendations and indicated they have initiated or planned to initiate corrective action.

## Background

The District serves the Towns of Independence and Willing in Allegany County and the Town of West Union in Steuben County. The District is governed by an elected five-member Board of Education (Board). The Board is responsible for the general management and control of financial and educational affairs.

The Superintendent of Schools is the chief executive officer responsible, along with other administrative staff, for day-to-day management under the Board's direction.

The District's Junior Accountant (Accountant) is responsible for managing access to the network and information systems, among his other duties.

| Quick Facts | |
|---|---|
| **Network User Accounts** | 268 |
| **Student Information System User Accounts** | 98 |
| **Financial System User Accounts** | 4 |
| **Enrollment** | 168 |
| **Employees** | 47 |

## Audit Period

July 1, 2019 – January 28, 2021

# Information Technology

The District relies on its IT assets for Internet access, email and for maintaining financial, personnel and student records and data. The District contracts with BOCES to provide IT services.

## Why Should the District Secure Access to the Network and Information Systems?

Computer networks, a group of two or more computers, can be accessed by network user accounts, and information systems can be accessed using application user accounts. Both types of user accounts identify specific users. Network user accounts provide access to resources on a network and are managed centrally by a server and/or domain controller.[1] Application user accounts provide users with access to resources within each information system, such as a financial system or a student information system, and are managed by the application server.

To minimize the risk of unauthorized network and application access, district officials should actively manage, network and software application user accounts, including their creation, use and dormancy, and regularly review them to ensure they are still needed.

Officials should have written procedures in place to grant, change and disable user permissions to the network and specific software applications. These procedures should establish who has the authority to grant or change user permissions and allow users to access only what is necessary to complete their job duties. User permissions should be updated as necessary and unneeded accounts should be disabled or removed in a timely manner.

Officials should have written procedures… to grant, change and disable user permissions to the network and specific software applications.

Because shared accounts are not assigned to a single user, officials may have difficulty managing these accounts and linking any suspicious activity to a specific user. To help ensure individual accountability, all users should have and use their own user account to gain access to a network and applications. If shared accounts are needed, officials should have procedures in place to monitor who uses the accounts and when they are used.

IT managers should set up user accounts with specific user permissions needed by each individual to perform their job functions. This ensures network access is restricted to only those individuals who are authorized to access it. Officials should review and approve user permissions before the IT manager configures user accounts with specific permissions, and this approval should be documented.

[1] A server is a computer equipped with specific programs that provide resources and data to other computers which are connected to the server. A domain controller is the main server computer in the domain (network) that controls or manages all computers within the domain.

## Officials Did Not Adequately Secure User Accounts and Permissions

Unnecessary Network Accounts – During our review of all network accounts, we found six unnecessary network user accounts. These included two network user accounts for individual users and four accounts that were shared or generic accounts. Three of these accounts were not accessed in the prior six months, and the other three accounts were never used to log into the network. District officials told us these accounts were needed for certain functions including email access and testing student access. Unnecessary user accounts that have not been disabled or removed could potentially be used by former employees or others for malicious purposes.

Shared Accounts – During our review of network accounts, we found 35 shared network user accounts that had varied purposes, ranging from administrative functions such as building controls, instructional purposes such as accounts for students to share, and accounts used to access servers and configure web filtering settings.

The Accountant told us all of these accounts were necessary. However, because of the large number of shared accounts, officials may have difficulty managing them and linking any suspicious activity to a specific user. Although officials told us these accounts were necessary, one account had not been used in the past six months. District officials told us this account was a backup account for another user in case of a technical issue.

In addition, officials did not have procedures in place to monitor who used the shared accounts. As a result, the District had a greater risk that personal, private and sensitive information could be changed intentionally or unintentionally or used inappropriately and officials would not be able to identify who performed the unauthorized activities.

Unnecessary Application User Permissions – We reviewed user permissions of all 98 application user accounts for the student information system and all four user accounts for the financial system. Although officials were unable to provide written job descriptions or duties, we found that user permissions for the student information system were appropriate.

However, the permissions granted to the four financial system users were more than necessary for their job responsibilities. Officials told us that due to the small size of the business office, users were cross-trained on other job functions and therefore required more permissions. However, officials should add or remove permissions, as needed, for these users' current job responsibilities.

…[T]he permissions granted to the four financial system users were more than necessary for their job responsibilities.

The District does not have a written user permissions policy or procedures to grant, modify and disable user permissions to the network or to specific software applications. Officials were unable to provide any evidence that permissions for either the student information system or the financial system were formally approved. In addition, the District did not regularly review user permissions for the network or applications to determine whether they were still needed.

The Accountant told us that BOCES was responsible for securing access to the network and information systems and ensuring best practices were used. BOCES officials told us that they update settings as indicated in the District's technology or security policy or when requested by the District. However, the District did not have written IT policies in place, other than the acceptable use policy (refer to our publication *IT Governance* for IT policies that are required and recommended). District officials told us they did not have these policies in place because District officials coordinated access to the system with BOCES and did not think they were needed. The Accountant told us in his absence BOCES would be responsible for managing access to the network and information systems.

In addition, (other than cooperative service agreements with BOCES) officials did not have a written agreement with BOCES that specified the District's needs and expectations and the level of service to be provided. Because officials did not adequately secure access to the network and information systems, the District had a greater risk that its computer resources could be misused or abused.

### What Do We Recommend?

The Board and District officials should:

1. Periodically review user accounts and ensure that unneeded user accounts are disabled.

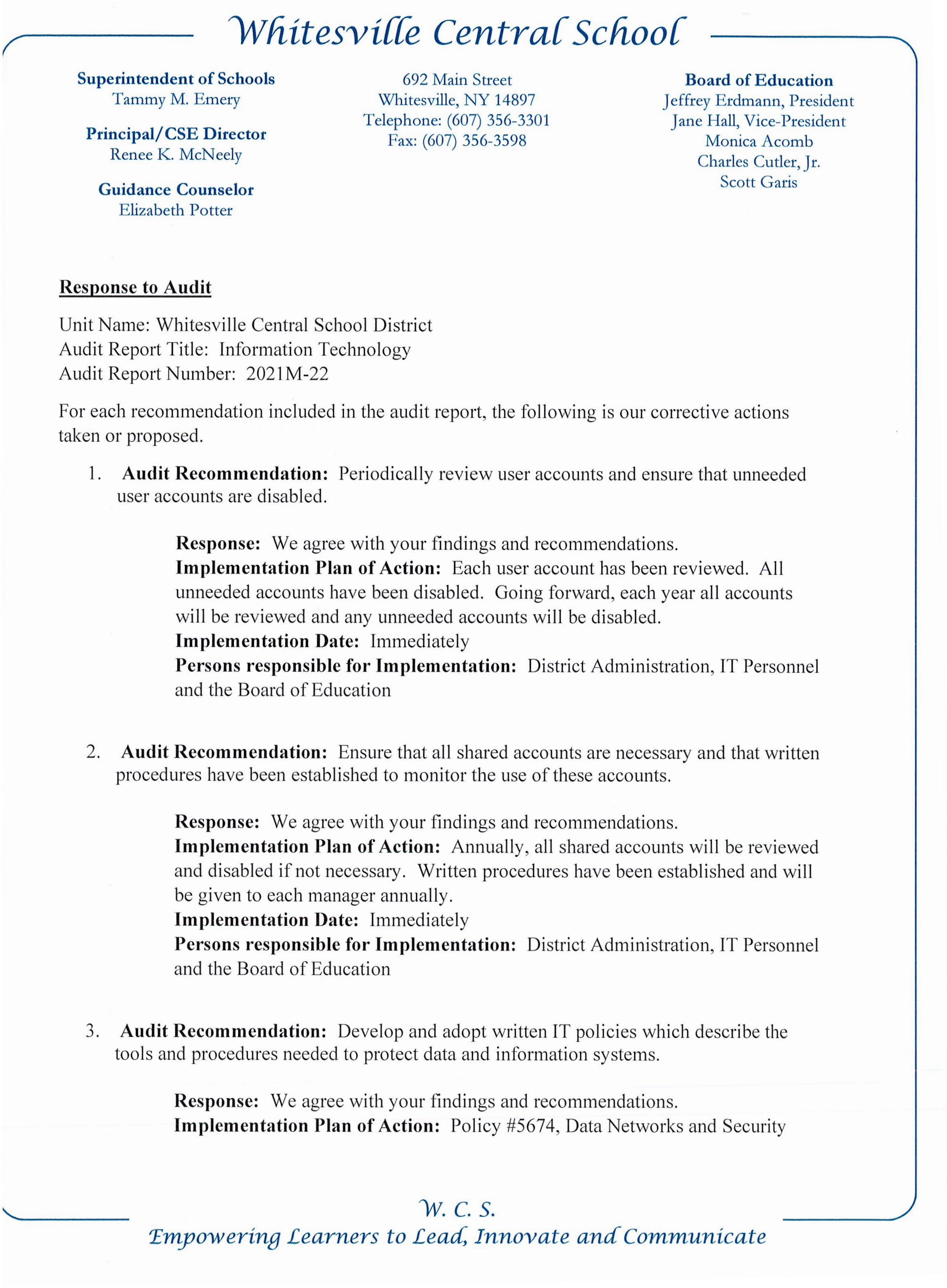
2. Ensure that all shared accounts are necessary and that written procedures have been established to monitor the use of these accounts.

3. Develop and adopt written IT policies which describe the tools and procedures needed to protect data and information systems.

4. Develop and adopt a written user permissions policy and develop comprehensive written procedures to add, modify and disable user permissions to the network and information systems.

5. Ensure that a written agreement with BOCES clearly states the District's needs and expectations and specifies the level of service to be provided.

# Appendix A: Response From District Officials



Whitesville Central School

**Superintendent of Schools**
Tammy M. Emery

**Principal/CSE Director**
Renee K. McNeely

**Guidance Counselor**
Elizabeth Potter

692 Main Street
Whitesville, NY 14897
Telephone: (607) 356-3301
Fax: (607) 356-3598

**Board of Education**
Jeffrey Erdmann, President
Jane Hall, Vice-President
Monica Acomb
Charles Cutler, Jr.
Scott Garis

**Response to Audit**

Unit Name: Whitesville Central School District
Audit Report Title: Information Technology
Audit Report Number: 2021M-22

For each recommendation included in the audit report, the following is our corrective actions taken or proposed.

1. **Audit Recommendation:** Periodically review user accounts and ensure that unneeded user accounts are disabled.

   **Response:** We agree with your findings and recommendations.
   **Implementation Plan of Action:** Each user account has been reviewed. All unneeded accounts have been disabled. Going forward, each year all accounts will be reviewed and any unneeded accounts will be disabled.
   **Implementation Date:** Immediately
   **Persons responsible for Implementation:** District Administration, IT Personnel and the Board of Education

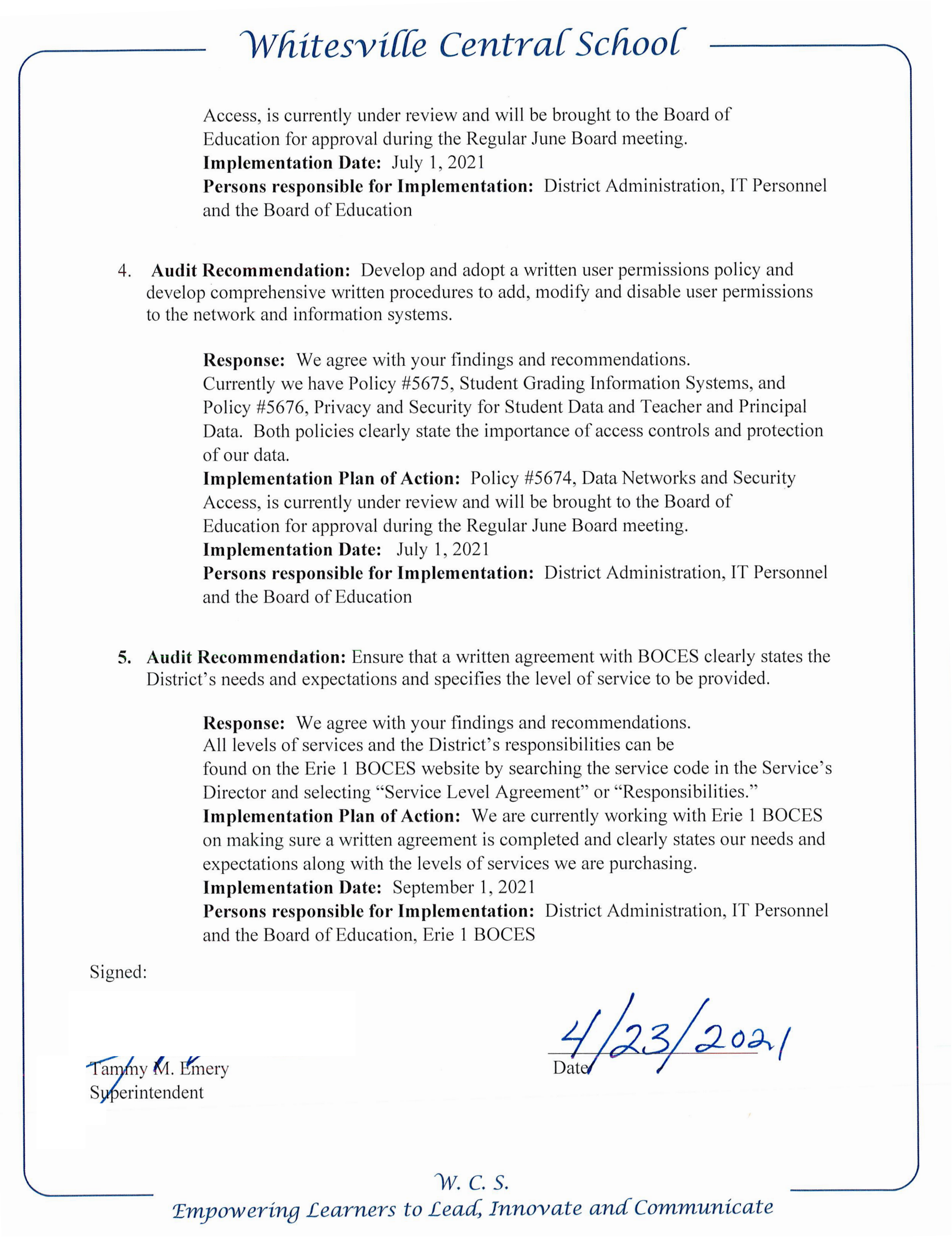
2. **Audit Recommendation:** Ensure that all shared accounts are necessary and that written procedures have been established to monitor the use of these accounts.

   **Response:** We agree with your findings and recommendations.
   **Implementation Plan of Action:** Annually, all shared accounts will be reviewed and disabled if not necessary. Written procedures have been established and will be given to each manager annually.
   **Implementation Date:** Immediately
   **Persons responsible for Implementation:** District Administration, IT Personnel and the Board of Education

3. **Audit Recommendation:** Develop and adopt written IT policies which describe the tools and procedures needed to protect data and information systems.

   **Response:** We agree with your findings and recommendations.
   **Implementation Plan of Action:** Policy #5674, Data Networks and Security

W. C. S.
Empowering Learners to Lead, Innovate and Communicate



Access, is currently under review and will be brought to the Board of Education for approval during the Regular June Board meeting.
**Implementation Date:** July 1, 2021
**Persons responsible for Implementation:** District Administration, IT Personnel and the Board of Education

4. **Audit Recommendation:** Develop and adopt a written user permissions policy and develop comprehensive written procedures to add, modify and disable user permissions to the network and information systems.

**Response:** We agree with your findings and recommendations.
Currently we have Policy #5675, Student Grading Information Systems, and Policy #5676, Privacy and Security for Student Data and Teacher and Principal Data. Both policies clearly state the importance of access controls and protection of our data.
**Implementation Plan of Action:** Policy #5674, Data Networks and Security Access, is currently under review and will be brought to the Board of Education for approval during the Regular June Board meeting.
**Implementation Date:** July 1, 2021
**Persons responsible for Implementation:** District Administration, IT Personnel and the Board of Education

5. **Audit Recommendation:** Ensure that a written agreement with BOCES clearly states the District's needs and expectations and specifies the level of service to be provided.

**Response:** We agree with your findings and recommendations.
All levels of services and the District's responsibilities can be found on the Erie 1 BOCES website by searching the service code in the Service's Director and selecting "Service Level Agreement" or "Responsibilities."
**Implementation Plan of Action:** We are currently working with Erie 1 BOCES on making sure a written agreement is completed and clearly states our needs and expectations along with the levels of services we are purchasing.
**Implementation Date:** September 1, 2021
**Persons responsible for Implementation:** District Administration, IT Personnel and the Board of Education, Erie 1 BOCES

Signed:

4/23/2021

Tammy M. Emery
Superintendent

Date

# Appendix B: Audit Methodology and Standards

We conducted this audit 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. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We interviewed District officials and reviewed the District's policy manual to determine the policies in place and to gain an understanding of IT operations, specifically those related to the granting, modifying and revoking of network user accounts.
- We provided the Accountant with a computerized audit script to run on the District's domain controller. We analyzed each report generated by the script to identify network user accounts and security settings that indicated ineffective IT controls.
- We compared the District's employee master and payroll list reports to names of all account users listed in the audit script report to determine whether all users with active network accounts were currently employed or contracted by the District.
- From various software permissions reports from the financial and student information systems we determined how user permissions were managed. We then examined the user permissions for all users to determine whether access was appropriate based on job duties.

Our audit also examined the adequacy of certain information technology controls. Because of the sensitivity of some of this information, we did not discuss the results in this report but instead communicated them confidentially to District officials.

We conducted this performance audit in accordance with generally accepted government auditing standards (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.

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.

The Board has the responsibility to initiate corrective action. 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, 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. 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 CAP should be posted on the District's website for public review.

# Appendix C: Resources and Services

**Regional Office Directory**
www.osc.state.ny.us/sites/default/files/local-government/documents/pdf/2018-12/regional_directory.pdf

**Cost-Saving Ideas** – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263196&issued=All

**Fiscal Stress Monitoring** – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

**Local Government Management Guides** – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263206&issued=All

**Planning and Budgeting Guides** – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

**Protecting Sensitive Data and Other Local Government Assets** – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/sites/default/files/local-government/documents/pdf/2020-05/cyber-security-guide.pdf

**Required Reporting** – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/local-government/required-reporting

**Research Reports/Publications** – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263211&issued=All

**Training** – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/local-government/academy

## Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

www.osc.state.ny.us/local-government

Local Government and School Accountability Help Line: (866) 321-8503

**BUFFALO REGIONAL OFFICE** – Jeffrey D. Mazula, Chief Examiner

295 Main Street, Suite 1032 • Buffalo, New York 14203-2510

Tel (716) 847-3647 • Fax (716) 847-3643 • Email: Muni-Buffalo@osc.ny.gov

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

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller