THOMAS P. DiNAPOLI
COMPTROLLER

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER
110 STATE STREET
ALBANY, NEW YORK 12236

ROBIN L. LOIS, CPA
DEPUTY COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY
Tel: (518) 474-4037 Fax: (518) 486-6479

November 2025

Dr. Vincent Butera, Superintendent
Members of the Board of Education
Hunter-Tannersville Central School District
6094 Main Street, P.O. Box 1018
Tannersville, NY 12485

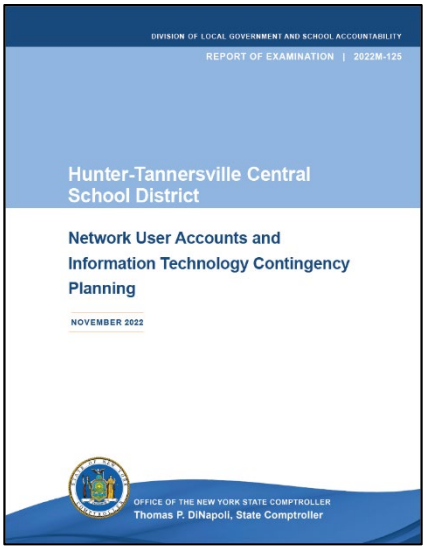
Report Number: 2022M-125-F

Dear Superintendent Butera and Members of the Board of Education:

One of the Office of the State Comptroller's (OSC's) primary objectives is to identify areas where school district officials can improve their operations and provide guidance and services that will assist them in making those improvements. OSC also works to develop and promote short-term and long-term strategies to enable and encourage officials to reduce costs, improve service delivery and to account for and protect their assets.

In accordance with these objectives, we conducted an audit of the Hunter-Tannersville Central School District (District) to assess the District's network user accounts and information technology contingency planning. As a result of the audit, we issued a report, dated November 2022, identifying certain conditions and opportunities for the District Board of Education's (Board), officials' and Director of Technology's review and consideration (Figure 1).

Figure 1: Hunter-Tannersville Central School District 2022 OSC Audit Report



https://www.osc.ny.gov/files/local-government/audits/2022/pdf/hunter-tannersville-central-school-district-2022-125.pdf

In response to the audit, officials filed a corrective action plan (CAP) with OSC on October 28, 2022. The CAP identified the actions officials took or planned to take to implement the audit recommendations.

To further our policy of providing assistance to local governments and school districts, we revisited the District in June 2025 to review progress in implementing the audit's recommendations. The follow-up review was limited to interviews with District personnel and inspection of certain data

and documents related to the issues identified in the report and review of the District's CAP[1] and confidential communications with District officials.[2]

Of the five recommendations contained in the public audit report, we determined, based on our limited procedures, that the District's Director of Technology, Board and officials fully implemented all five recommendations. We also reviewed progress in implementing the recommendations related to the sensitive IT control weaknesses that we reported to officials confidentially, and communicated those results confidentially to District officials.

Recommendation 1 – Network User Account Procedures

The Director of Technology should develop and communicate comprehensive written procedures for managing and monitoring nonstudent network user account access that ensure network user accounts are disabled once they are no longer needed.

Status of Corrective Action: Fully Implemented

Observations/Findings: Subsequent to the audit, the Director of Technology developed checklists that outline procedures to manage and monitor nonstudent network user account access. The checklists address network user accounts for new employees, employees separated from the District, employees transferring between District departments, and non-employee user accounts. The checklists outline the Director of Technology's responsibilities for nonstudent network user account creation, access removal and role-based changes. The Director of Technology told us he communicated the procedures to the staff responsible for personnel changes to help ensure appropriate and timely notification of personnel changes and network user account access update needs. As noted in Recommendation 2, our testing determined all nonstudent network user accounts enabled as of August 2025 were needed and appropriate for authorized network users and IT services.

Recommendation 2 – Unneeded Network User Accounts and Authorized Account List

The Director of Technology should disable network user accounts of former employees and other users as soon as they are no longer needed and maintain and periodically evaluate a list of authorized nonstudent network user accounts.

Status of Corrective Action: Fully Implemented

Observations/Findings: We obtained and reviewed a list of nonstudent network user accounts enabled as of August 2025 and determined all 140 enabled accounts were for current District employees and necessary IT services. In addition, the Director of Technology told us that, subsequent to the audit, he began reviewing network user accounts at the end of each school year and any time an employee started or separated from District employment. Our review of the Director of Technology's October 2024 and January 2025 work log confirmed that he reviewed nonstudent network user accounts. Additionally, he told us he spot-checked nonstudent network

1 See Appendix A for the District's CAP to the OSC audit report.
2 The audit also examined the adequacy of certain sensitive IT controls. Because of the sensitivity of some of this information, we did not discuss the results in our audit report, but instead communicated them confidentially to District officials.

user accounts when a password needed to be reset, at which time he disabled any account he deemed unnecessary.

Recommendation 3 – Unique Network User Accounts or Shared and Service Account Monitoring Procedures

The Director of Technology should ensure all network users have and use their own unique network user accounts to access the District's network or develop procedures to monitor shared and service accounts as to who uses the accounts and when and how they are used.

Status of Corrective Action: Fully Implemented

Observations/Findings: Based on our review of the District's nonstudent network user account list, we determined that District records indicate that network users had and used their own unique network user accounts to access the District's network. Additionally, subsequent to the audit, the Director of Technology created a shared accounts procedure for monitoring shared accounts. The procedure included disabling all shared accounts at the end of each school year and re-enabling only upon a formal request. As of August 2025, shared account use was limited to elementary classrooms, where students did not have or need individual network access. Additionally, subsequent to the audit, the Director of Technology developed an internal checklist that outlined procedures to manage and monitor service accounts. The checklist outlined the Director of Technology's responsibilities for service account creation, removal and monitoring.

Recommendation 4 – Written IT Contingency Plan

The Board and District officials should develop and adopt a comprehensive written IT contingency plan and ensure it is periodically tested, updated and distributed to all key officials.

Status of Corrective Action: Fully Implemented

Observations/Findings: The Board adopted a Data Networks and Security Access policy (policy)in August 2024. The policy required IT staff to plan, implement and monitor IT security mechanisms, procedures and technologies necessary to prevent improper or illegal disclosure, modification or denial of sensitive information in the District computer system. As such, the Director of Technology developed a comprehensive written IT contingency plan in June 2024 in accordance with the policy.

The Director of Technology told us, and the Superintendent confirmed, that he distributed the IT contingency plan to the recipients listed within it in November 2024. The Director of Technology reviewed and updated the plan annually. We reviewed the Director of Technology's October 2024 work log and confirmed the Director of Technology updated the IT contingency plan accordingly. The Director of Technology and District officials also told us that they complete tabletop exercises (discussion-based simulations of IT incidents or disruptions) annually to test the efficacy of the plan, and they update the plan as needed based upon the discussions and results.

Recommendation 5 – Backup Data Storage and Testing

The Board and District officials should store backup data at a secure off-site location, ensuring the data is maintained off-network, encrypted and routinely tested to ensure its integrity.

Status of Corrective Action: Fully Implemented

Observations/Findings: The Director of Technology told us that backup data was stored at a secure off-site location, and the data is off-network and encrypted. Subsequent to the audit, the Director of Technology developed backup procedures for testing and restoring backup data to help ensure backups function as intended. We reviewed worklogs and documentation showing backups were successfully restored and confirmed the Director of Technology tested the backup data's integrity monthly.

During the review, we discussed the basis for the recommendations and the operational considerations relating to these issues.

Thank you for the courtesies and cooperation extended to our auditors during this review. If you have any further questions, please contact Jennifer Kenneson, Chief Information Systems Auditor, at (518) 738-2639.

Sincerely,

Robin L. Lois, CPA
Deputy Comptroller

Appendix A – District's' CAP to the OSC Audit Report

Hunter-Tannersville Central School District
Office of the Superintendent
6094 Main Street, P.O. Box 1018, Tannersville, N.Y. 12485
518-589-5400 Ext. 1000 www.htcschools.org

October 28, 2022

Office of the State Comptroller
Division of Local Government and School Accountability
Chief Examiner, Dara Disko-McCagg
Newburgh Regional Office
33 Airport Center Driver, Suite 103
New Windsor, New York 12553

Re: Hunter-Tannersville CSD
Network User Accounts & Information Technology Contingency Planning
Audit Period - July 1, 2020 - July 27, 2021
Audit Report Number - 2022M-125

Dear Chief Examiner Disko-McCagg,

Hunter-Tannersville CSD has received the Draft Audit Report titled Network User Accounts & Information Technology Contingency Planning.

The Board of Education, District Administration, and the Director of Technology appreciate the thorough work and recommendations provided by the Office of the State Comptrollers. Recognizing that technology continues to demonstrate rapid growth and expansion into all school district functions is essential. Thus creating more vulnerabilities for school districts. The OSC audit team has provided the district with strategic recommendations to support our ability to mitigate cyber-attacks.

Before the audit began, Hunter-Tannersville recognized the urgency to improve our IT controls to protect district assets and confidential data. We began collaborating with the Capital Region BOCES Cyber and Vendor Risk Management service designed to identify, mitigate, and manage cyber risks. For several months now, HTC has been working with Capital Region BOCES, who are providing the following services to the district:

Board of Education
Bobbi Schmitt, President
Barbara Bates, Vice President
Andrea Benjamin-Legg
Andrew Poladian
Courtney Brady

- **IT Risk Assessment** — Analysis is centered on publicly-accessible systems that can be observed from the internet.
- **Board IT Policy Review** — We will review Board IT policies against current federal and state requirements and will provide recommendations for each policy and where deemed appropriate.
- **General Liability and Cyber Insurance Review** — At the organization's discretion, we will develop and facilitate the process for an insurance RFP and/or a review of your current cyber liability insurance.
- **Compliance Analysis with Industry, Federal and State Standards** — Using a number of online assessment tools, a gap analysis will be conducted, and an action plan created to assist the organization in increasing their level of compliance. Project Management support will be provided throughout the agreement to implement the action plan.
- **Training and Advisement, Including Awareness and Incident Response Training** — We will provide training materials and guidance related to awareness and incident response training. The training and guidance provide staff with the knowledge, skills and resources regarding data, cyber security, vendor risk management and responding to a cyber security incident.
- **Vendor Risk Vetting** — An assessment and recommendation will be conducted on vendors which the organization would like to engage with. The assessment will be based on information provided by the vendor regarding their compliance with New York State Education Law 2-d and NIST CSF compliance.
- **Facilitate Data Privacy Agreements**

The correction action plan (CAP), represented in the table below, outlines our agreement with OSC and our specific improvement plan. We believe that our CAP and the additional Cyber Risk and Vendor Management service support will provide the district with a robust plan to mitigate threats.

Recommendations	Agree or Disagree	Intended Actions	Person Responsible
Recommendation #1: Develop and communicate comprehensive written procedures for managing and monitoring nonstudent network user account access that ensure network	Agree	**District Response:** The unneeded accounts have been removed. The district office and IT Director have worked on the processes in place for notifying each other of staff changes. They have put checklists together for when an employee enters or leaves the district. A plan is also	District Office & IT Director w/ support from the NERIC Cybersecurity Risk Team

Board of Education
Bobbi Schmitt, President
Barbara Bates, Vice President
Andrea Benjamin-Legg
Andrew Poladian
Courtney Brady

user accounts are disabled once they are no longer needed.		being formulated for conducting regular reviews of network accounts annually. The district is currently working with the NERIC Cybersecurity Risk service on properly documenting IT procedures and policies.	
Recommendation #2: Disable network user accounts of former employees and other users as soon as they are no longer needed and maintain and periodically evaluate a list of authorized nonstudent network user accounts.	Agree	**District Response:** The unneeded accounts have been removed. The district office and IT Director have worked on the processes in place for notifying each other of staff changes. They have put checklists together for when an employee enters or leaves the district. A plan is also being formulated for conducting regular reviews of network accounts annually. The district is currently working with the NERIC Cybersecurity Risk service on properly documenting IT procedures and policies.	District Office & IT Director w/ support from the NERIC Cybersecurity Risk Team
Recommendation #3 Ensure all network users have and use their own unique network user accounts to access the District's network or develop procedures to monitor shared and service accounts as to who uses the accounts and when and how they are used.	Agree	**District Response:** The majority of staff and students have their own network accounts. For the grade levels where there are class accounts a process is being documented for monitoring them.	IT Director

Board of Education
Bobbi Schmitt, President
Barbara Bates, Vice President
Andrea Benjamin-Legg
Andrew Poladian
Courtney Brady

Recommendation #4: Develop and adopt a comprehensive written IT contingency plan and ensure it is periodically tested, updated and distributed to all key officials.	Agree	**District Response:** The district is also working with the NERIC Cybersecurity Risk service to improve on the district's IT contingency plan.	District Office & IT Director w/ support from the NERIC Cybersecurity Risk Team
Recommendation #5 Store backup data at a secure off-site location, ensuring the data is maintained off-network, encrypted and routinely tested to ensure its integrity.	Agree	**District Response:** The district is also working with the NERIC Cybersecurity Risk service to improve on the district's back strategy	District Office & IT Director w/ support from the NERIC Cybersecurity Risk Team

[redacted]

~~Bobbi~~ Schmitt
Board of Education President

Board of Education
Bobbi Schmitt, President
Barbara Bates, Vice President
Andrea Benjamin-Legg
Andrew Poladian
Courtney Brady