THOMAS P. DiNAPOLI
COMPTROLLER

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

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

March 2026

Michael R. Eiffe, Superintendent
Members of the Board of Education
Chittenango Central School District
1732 Fyler Road
Chittenango, NY 13037

Report Number: 2023M-155-F

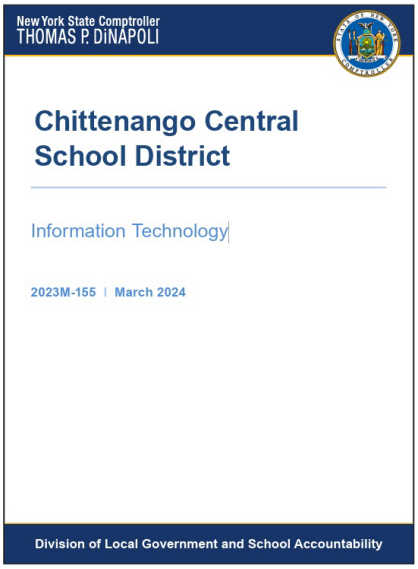
Dear Superintendent Eiffe and Members of the Board of Education:

One of the Office of the New York State Comptroller's (OSC) 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 school district officials to reduce costs, improve service delivery and to account for and protect their school district's assets.

According to these objectives, we conducted an audit of the Chittenango Central School (District) to assess the District's information technology (IT).

As a result of the audit, we issued a report, dated March 2024, identifying certain conditions and opportunities for District management's review and consideration (Figure 1). In response to the audit, District officials filed a corrective action plan (CAP) with OSC on May 22, 2024.[1] The CAP identified the actions District officials took or planned to take to implement the audit recommendations.

**Figure 1: Chittenango Central School District 2024 Audit Report**




https://www.osc.ny.gov/files/local-government/audits/2024/pdf/chittenango-central-school-district-2023-155.pdf

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

1 See Appendix A for the District's CAP to the OSC audit report.

inspecting certain data and documents related to the issues identified in our report, confidential communications with District officials[2] and a review of the District's CAP.

Of the four recommendations contained in the 2023M-155 report, we determined, based on our limited procedures, that the Board of Education (Board), District officials and the Director of Technology (Director) partially implemented two recommendations and did not implement two recommendations. As a result, the District continued to have an increased risk that its IT system and personal, private and sensitive information (PPSI)[3] could be accessed by unauthorized users. The District could also lose important data and suffer a serious interruption to operations that depend on its computerized environment, such as not being able to process checks to pay vendors or employees or process student grades. 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 – IT Contingency Plan**

The Board and District officials should develop and adopt a written IT contingency plan, update the plan as needed and distribute it to all responsible parties.

Status of Corrective Action: Partially Implemented

Observations/Findings: As of October 2025, the Chief Financial Officer (CFO) was in the process of developing an IT contingency plan in coordination with the District's IT support provider, Central New York Regional Information Center (CNYRIC). The CFO told us that coordinating with CNYRIC should help the District ensure the procedures in their plan align with required privacy standards, security best practices, and recommended guidelines for protecting critical systems and data. However, the Board President told us the plan was not yet presented to the Board for adoption because it was incomplete. The IT contingency plan addressed key individuals needed to resume operations but did not include all relevant details including, for example, the hardware needed in case of sudden unplanned disruptions. Rather, the plan had a placeholder to insert such details, and it was not completed.

Without a complete and Board-adopted IT contingency plan, the District continued to have an increased risk that it could lose important data and suffer a serious interruption to operations that depend on its computerized environment, such as not being able to process checks to pay vendors or employees or process student grades.

**Recommendation 2 – Network and Local User Account Procedures**

The Director should ensure written procedures for granting, verifying, changing and disabling network and local user accounts are established and followed.

2 The audit also examined the adequacy of certain sensitive IT controls. Because of the sensitivity of some of this information, we communicated it confidentially to District officials.

3 PPSI is any information to which unauthorized access, disclosure, modification or destruction – or disruption of access of use – could have or cause a severe impact on critical functions, employees, customers (students), third parties or other individuals or entities.

Status of Corrective Action: Not Implemented

Observations/Findings: The Director did not ensure written procedures were established and followed for granting, verifying, changing and disabling network and local user accounts. Because the District implemented an automated syncing process in August 2025, between the District's Human Resources (HR) system and central network management tool, the Director believed that written procedures were not immediately necessary. However, developing documented procedures could help the Director establish who has the authority to grant or change user account access and require District officials to periodically review enabled user accounts to ensure they are appropriate and authorized. Until the Director establishes written procedures for network and local user accounts, the District will continue to have an increased risk that its IT system and PPSI may be accessible to unauthorized users.

**Recommendation 3 – Unneeded Nonstudent Network and Local User Accounts**

The Director should disable the unneeded nonstudent network and local user accounts identified in this report and ensure future user accounts are disabled as soon as they are no longer needed.

Status of Corrective Action: Partially Implemented

Observations/Findings: We obtained and reviewed a list of enabled nonstudent network user accounts and determined all 89 network user accounts identified as unnecessary during the 2024 OSC audit were disabled as of October 2025. However, we determined during our review that 44 of the 584 enabled nonstudent network user accounts were unnecessary as of October 2025, and District officials should have disabled them. The 44 accounts were associated with former employees, other users who no longer needed network access, or duplicate creations that were not disabled in a timely manner. The Director said the 44 unnecessary accounts were not disabled because the accounts' users were not in the District's HR system and, as such, the accounts were not automatically disabled as expected when they became unnecessary.

Using our professional judgment based on the computers' operating system versions and assigned users' employee status as of October 2025, we reviewed the local user accounts enabled on three of the 12 user computers sampled during the 2024 OSC audit. Of the seven local user accounts enabled on the three computers as of October 2025, we determined that four were identified as unnecessary during the 2024 OSC audit and the remaining three local user accounts were authorized and necessary. The IT Director told us the four unnecessary local accounts had not yet been disabled because he planned to upgrade the computers soon.

Because the Director did not ensure network and local user accounts were disabled as soon as they were no longer needed, the District's PPSI and IT resources continued to have an increased risk for inappropriate access and could be compromised through the additional entry points that remained enabled.

**Recommendation 4 – Periodic Network User Account and Administrative Permissions Review**

The Director should establish and implement a system to periodically review all existing network user accounts and administrative permissions to determine whether they are needed and properly disable those that are deemed unneeded.

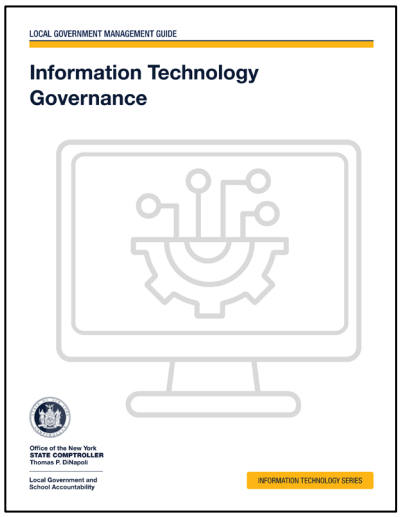
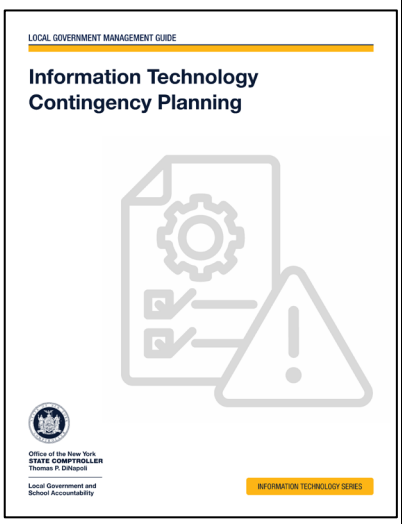
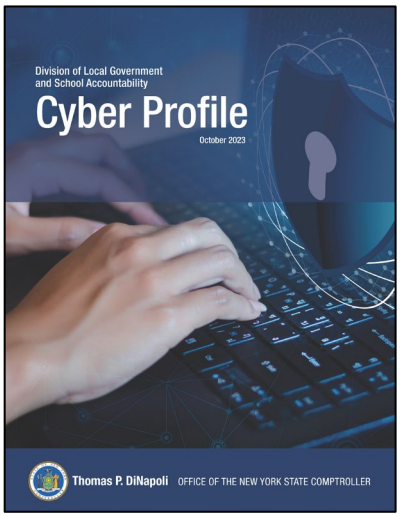
Status of Corrective Action: Not Implemented

Observations/Findings: The Director did not establish and implement a system to periodically review existing network user accounts and administrative permissions. As noted in Recommendation 2, the District implemented an automated syncing process in August 2025, between the District's HR system and central network management tool. District officials indicated that they are in the process of identifying and addressing deficiencies within the syncing process before they establish and implement an account and permissions review system. However, the Director may have identified the unnecessary network user accounts noted in Recommendation 3 and been better equipped to disable the accounts prior to our inquiry, had an account and permissions review system been established and implemented in a timelier manner. As a result, the District continued to have an increased risk that its IT system and PPSI could be accessed by unauthorized users.

During our review, we discussed the basis for our recommendations and the operational considerations relating to these issues. We encourage the Board, District officials and Director to continue their efforts to fully implement our recommended improvements. For additional guidance, the Board, District officials and Director should refer to OSC's *Local Government Management Guides*: *Information Technology Governance* and *Information Technology Contingency Planning*, as well as our publication *New York Local Government and School Cybersecurity: A Cyber Profile*, which are available on our website (Figure 2).

**Figure 2: OSC Publications**

OSC *Local Government Management Guides* and other informational resources are available on our website to help officials understand and perform their responsibilities and implement effective internal controls.

| *Information Technology Governance* | *Information Technology Contingency Planning* | *New York Local Government and School Cybersecurity: A Cyber Profile* |
|---|---|---|
|  |  |  |
| https://www.osc.ny.gov/files/local-government/publications/pdf/information-technology-governance.pdf | https://www.osc.ny.gov/files/local-government/publications/pdf/itcontingencyplanning.pdf | https://www.osc.ny.gov/files/localgovernment/publications/pdf/nys-localgov-school-cyber-profile.pdf |

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 for the OSC Audit Report**


# Chittenango Central School District

Scott P. Mahardy
Ass't. Superintendent for Business
315-687-2850


5/21/2024

Office of the State Comptroller
Division of Local Government and School Accountability
State Office Building, Room 409
333 East Washington Street
Syracuse, NY 13202

Unit Name: Chittenango Central School District
Audit Report Title: Information Technology
Audit Report Number: 2023M-155

The Chittenango Central School previously received and reviewed the Draft Audit Report of Examination for the period covering July 1, 2021 – August 9, 2023. The district has previously submitted the above referenced acknowledgement to your office. We are pleased to provide our corrective action items in response to the audit findings.

**Audit Finding #1**
"The district did not adequately manage nonstudent network and local user accounts and permissions".

**Corrective Action**
At the close of the audit, all accounts have been reviewed and updated accordingly. The district has implemented an employee checklist both for entry and exit of employment. The checklist was developed in collaboration with our Human Resources Department, the Director of Technology, and the Superintendent's Office.. A bi-monthly review of accounts will be conducted.

**Responsible Parties**
The Director of Technology and the Assistant Superintendent for Business.

**Implementation date**
The above actions are ongoing.

**Audit Finding # 2**
"The Board and District Officials did not develop and adopt an IT Contingency Plan".

**Corrective Action**

The District will continue to work and develop a written IT contingency plan. Phase one (1) of the process was to implement a tape back-up system. The District will continue to consult with the CNYRIC for best practices in the development of an IT contingency plan and corresponding testing.

**Implementation date**

Tape back-up system completed 3/1/24. Balance of plan will be 7/1/24. Testing and revisions will be ongoing.

**Responsibility**

The Assistant Superintendent for Business, Director of Technology, and the Board of Education.

Respectfully,

Scott P. Mahardy
Assistant Superintendent for Business May 21
CAP approved by Board of Education ~~April 17~~, 2024