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

THOMAS P. DiNAPOLI
COMPTROLLER

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

September 2025

Adam VanDerStuyf, Superintendent
Members of the Board of Education
North Salem Central School District
230 June Road
North Salem, NY 10560

Report Number: 2022M-140-F

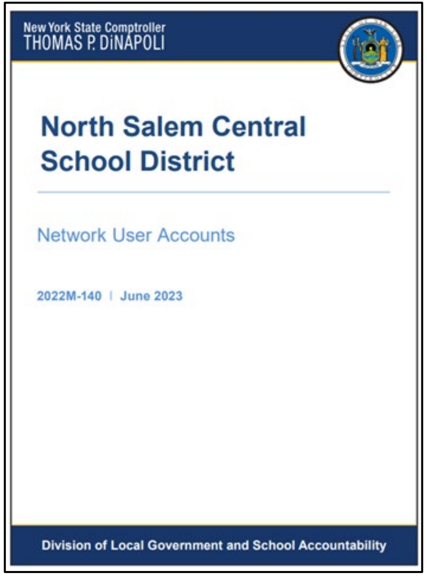
Dear Superintendent VanDerStuyf and Members of the Board of Education:

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 North Salem Central School District (District) to assess the District's network user accounts. As a result of our audit, we issued a report, dated June 2023, identifying certain conditions and opportunities for the District officials', Information Technology (IT) Director's and IT staff's review and consideration (Figure 1).

In response to the audit, officials filed a corrective action plan (CAP) with OSC on August 24, 2023. The CAP identified the actions officials took or planned to take to implement the audit recommendations.

Figure 1: North Salem Central School District 2023 OSC Audit Report



New York State Comptroller
THOMAS P. DiNAPOLI

North Salem Central School District

Network User Accounts

2022M-140 | June 2023

Division of Local Government and School Accountability

https://www.osc.ny.gov/files/local-government/audits/2023/pdf/north-salem-central-school-district-2022-140.pdf

To further our policy of providing assistance to local governments and school districts, we revisited the District in May 2025 to review progress in implementing our recommendations. Our follow-up review was limited to interviews with District personnel and inspection of certain documents related to the issues identified in our report and our confidential communications with District officials.[1]

[1] Our 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.

We reviewed progress in implementing our recommendations related to the sensitive IT control weaknesses that we communicated confidentially to District officials, and we also communicated our review result confidentially to District officials. In addition, of the three recommendations contained in the 2022-M-140 report, we determined, based on our limited procedures, that District officials, the IT Director and IT staff fully implemented one recommendation and partially implemented two recommendations. Until all recommendations are fully implemented, the District's network user accounts will continue to have an increased risk of being compromised.

Recommendation 1 – Develop Network User Account Procedures

Develop adequate procedures for granting, changing and disabling network user accounts. To help ensure that employees implement and comply with the procedures, the procedures should be in writing and distributed to applicable staff.

Status of Corrective Action: Fully Implemented

Observations/Findings: In July 2024, District officials revised the written procedures they developed for granting, changing and disabling network user accounts. We reviewed these procedures and determined they adequately outlined how network user accounts are automatically created, disabled and changed. The procedures also addressed a monthly manual review to help ensure user accounts are properly disabled by the automated system. More specifically, the Technology and Human Resources Departments maintained a spreadsheet of all active employees as a user list to cross reference against current enabled network user accounts. We interviewed the IT Director, IT staff, and third-party IT contractors who were responsible for implementing and complying with the procedures and determined each was aware of and understood the procedures. We also confirmed they updated the user list and performed monthly reviews in comparison with enabled network user accounts.

Recommendation 2 – Ensure Automated System Operation

Ensure that the automated system for disabling user accounts is operating properly.

Status of Corrective Action: Partially Implemented

Observations/Findings: District officials use an automated system for disabling network user accounts. This system automatically disables employees' network user accounts upon the District's Human Resources Department changing the employee status to "not active." While our review determined the automated system generally operated properly, it did not operate properly in all instances.

We reviewed all 328 enabled nonstudent network user accounts as of May 2025 and determined District officials should have disabled six user accounts (2 percent) for former employees. The six user accounts were not disabled by the automated system due to a software licensing error that occurred in the current year (2025) and caused the automated system not to complete its process. Further, while IT staff identified the six unneeded user accounts during a subsequent manual review prior to our audit follow up and made a log entry in the manual review audit log indicating the accounts were disabled, our review found these six accounts were still enabled. IT staff could not definitively state whether the log entry was a human error (i.e., incorrectly noted the six accounts as disabled), or whether the accounts were manually disabled and then subsequently re-enabled. Upon our inquiry, IT staff disabled the six unneeded network user accounts.

When former employees' network user accounts are not disabled in a timely manner, there is an increased risk of unauthorized access because any account on a network is a potential entry point for attackers. Former employees' network user accounts are of particular risk because they could potentially be used by those individuals or others for malicious activities without timely detection.

Recommendation 3 – Evaluate and Disable Unneeded Network User Accounts

Maintain a list of authorized user accounts and routinely evaluate and disable any unneeded network user accounts in a timely manner.

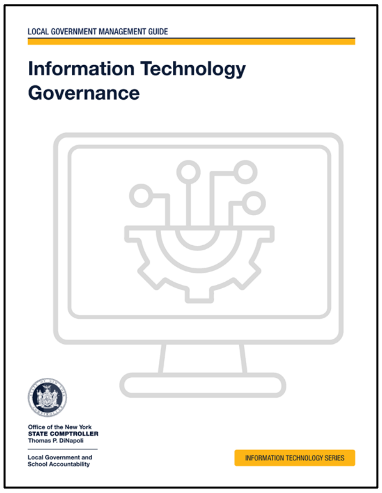
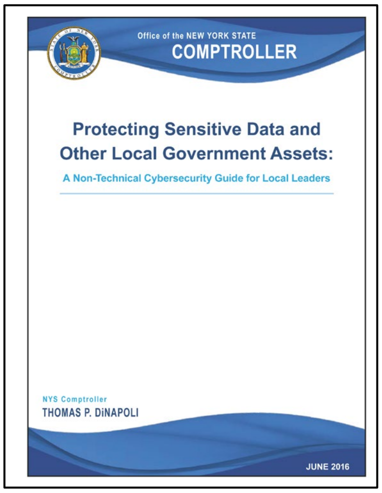
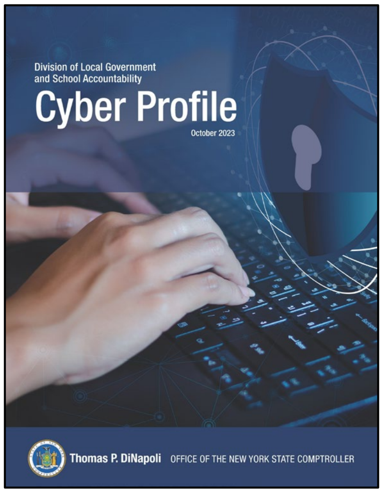
<u>Status of Corrective Action</u>: Partially Implemented

<u>Observations/Findings</u>: We reviewed and confirmed that District officials have established and maintained an up-to-date list of authorized network user accounts and performed monthly manual reviews. While District officials generally disabled unneeded network user accounts in a timely manner, not all unneeded network user accounts were disabled.

By automatically disabling most unneeded network user accounts, District officials were generally able to address the remaining accounts requiring manual action, such as accounts assigned to contractors or for temporary purposes, in a timely manner. To address these accounts, in July 2024, the District's IT Director and IT staff implemented a monthly manual review to identify and disable any remaining unneeded network user accounts. As noted in Recommendation 2, six former employee user accounts were still enabled as of May 2025. When unneeded network user accounts remain enabled, they are at an increased risk of being compromised.

During our review, we discussed the basis for our recommendations and the operational considerations relating to these issues with District officials. We encourage the District's officials, IT Director and IT staff to continue their efforts to fully implement our recommended improvements. For additional guidance, the District's officials, IT Director and IT staff should refer to OSC's *Local Government Management Guide*: *Information Technology Governance*, as well as our publications *Protecting Sensitive Data and Assets: A Non-Technical Cybersecurity Guide for Local Leaders* and *New York Local Government and School Cybersecurity: A Cyber Profile*, which are available on our website (Figure 2).

Figure 2: OSC Local Government Management Guide and Publications

Information Technology Governance	*Protecting Sensitive Data and Other Local Government Assets: A Non-Technical Cybersecurity Guide for Local Leaders*	*New York Local Government and School Cybersecurity: A Cyber Profile*
 LOCAL GOVERNMENT MANAGEMENT GUIDE Information Technology Governance Office of the New York STATE COMPTROLLER Thomas P. DiNapoli Local Government and School Accountability INFORMATION TECHNOLOGY SERIES	 Office of the NEW YORK STATE COMPTROLLER Protecting Sensitive Data and Other Local Government Assets: A Non-Technical Cybersecurity Guide for Local Leaders NYS Comptroller THOMAS P. DiNAPOLI JUNE 2016	 Division of Local Government and School Accountability Cyber Profile October 2023 Thomas P. DiNapoli OFFICE OF THE NEW YORK STATE COMPTROLLER
https://www.osc.ny.gov/files/local-government/publications/pdf/information-technology-governance.pdf	https://www.osc.ny.gov/files/local-government/publications/pdf/cyber-security-guide.pdf	https://www.osc.ny.gov/files/local-government/publications/pdf/nys-local-gov-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