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

September 2025

Dr. Sean Croft, Superintendent
Members of the Board of Education
Starpoint Central School District
4363 Mapleton Road
Lockport, NY 14094

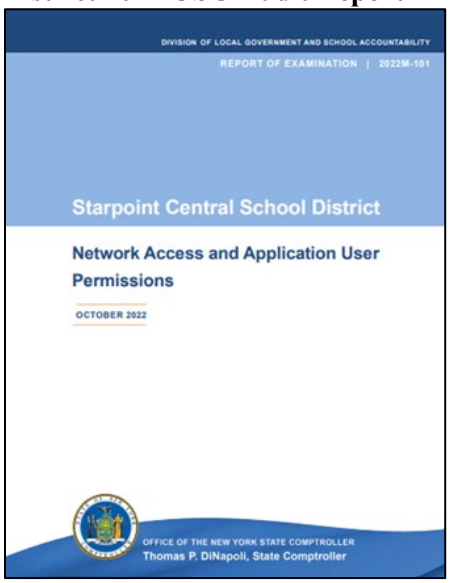
Report Number: 2022M-101-F

Dear Dr. Croft 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 Starpoint Central School District (District) to assess the District's network access and application user permissions. As a result of our audit, we issued a report, dated October 2022, identifying certain conditions and opportunities for District management's review and consideration (Figure 1). In response to the audit, officials filed a corrective action plan (CAP) with OSC on January 19, 2023. The CAP identified the actions officials took or planned to take to implement the audit recommendations.

Figure 1: Starpoint Central School District 2022 OSC Audit Report



https://www.osc.ny.gov/files/local-government/audits/2022/pdf/starpoint-central-school-district-2022-101.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 data and documents related to the issues identified in our report and our confidential communications with District officials. While we reviewed progress in implementing our recommendations related to sensitive IT control weaknesses, which we communicated confidentially to District officials, based on our limited procedures, we determined that the Board of Education (Board), District officials,

and the Network Manager and District-assigned BOCES[1] Coordinator (IT Managers) fully implemented one recommendation, partially implemented three recommendations, and did not implement one recommendation. As a result, the District's network and financial and student information applications continued to have increased opportunities for undetected malicious activities, improper access to students' private and personal information, and/or modification of accounting records to conceal malicious transactions.

Recommendation 1 – Develop User Permissions Policy and Procedures

Develop and adopt a written user permissions policy and develop comprehensive written procedures detailing the process to add, modify and disable user permissions to the network and applications including identifying the employees responsible for these processes and for notifying the IT Department.

Status of Corrective Action: Fully Implemented

Observations/Findings: Subsequent to our audit, the IT Managers developed comprehensive written procedures to document their process for adding, modifying and disabling user permissions to the network and applications, including identifying the employees responsible for these processes and for notifying the IT Department. In January 2025, the Board adopted a written user permissions policy, which formalized the IT Managers' procedures. We determined the District's Board-adopted user permissions policy and the internal procedures were adequate to help secure network and application access by restricting user access to only those network and application resources and data needed for learning or to complete job duties and responsibilities.

The District's written procedures clearly identified the IT Department as responsible for adding, modifying and disabling user permissions. The procedures also identified the department managers, building supervisors, the Human Resources Office, data owners and application administrators as responsible for notifying the IT Department when permission changes are needed.

Recommendation 2 – Ensure User Permissions Policy and Procedures Awareness and Compliance

Ensure employees responsible for implementing the user permissions policy and procedures are aware of the policy and complying with it.

Status of Corrective Action: Partially Implemented

Observations/Findings: District officials told us that all requests for adding, modifying and removing user access are submitted using the District's Technology User Request Form (TURF), and that the TURF is regularly discussed during monthly District administrative meetings. While attendance at the administrative meetings was not recorded, department managers and building supervisors generally attended. We requested the agenda for any administrative meeting where the

1 The District has an educational services contract with Orleans/Niagara Board of Cooperative Educational Services (BOCES) that includes providing information technology support through Erie 1 BOCES.

user access process was discussed and officials provided two meeting agendas – for April 2024 and March 2025. We reviewed the provided agendas and determined that the process and usage of the TURF was on the agenda for both meetings.

Of the three District employees responsible to oversee the implementation of the user permissions policy and procedures, one told us they regularly attend the administrative meetings and the remaining two directly report to a regular meeting attendee. Additionally, we discussed the TURF process and usage with each of the three District employees and determined each clearly understood their responsibility for implementing the policy and procedures.

To confirm compliance with the user permissions policy and procedures, we obtained a list of all 54 employees who separated from the District and all TURF submissions between January 2023 and May 2025. We compared the separated employee list and TURF submissions for disabling employee user accounts to the list of network user accounts enabled as of May 2025:

- One network user account, assigned to an employee who separated from the District on February 18, 2025 and had a TURF to disable their account submitted on February 28, 2025, was recorded as being disabled on April 2, 2025 as part of the 2025 inactive accounts review conducted by District officials. However, our testing determined the account was enabled as of May 2, 2025. District officials could not provide an explanation for why the account was enabled. IT Managers should disable the account and investigate whether the account was compromised or used for unauthorized access.
- While network user accounts were not enabled as of May 2025, TURFs were not submitted for 40 of the 54 separated employees. Although the accounts were properly disabled, with six accounts being discovered during the 2025 inactive account review, District officials did not follow the documented procedures and could not provide an explanation for why TURFs were not submitted for these separating employees.

Without consistent compliance with the District's user permissions policy and procedures, District officials cannot be assured that unnecessary network user accounts will be disabled in a timely manner. Unnecessary network user accounts that remain enabled increase opportunities for users to make unauthorized or improper changes, improperly access private and personal information, and/or modify records to conceal malicious activity.

Recommendation 3 – Evaluate and Disable Unnecessary Network User Accounts

Periodically evaluate existing network user accounts and disable any unnecessary network user accounts.

Status of Corrective Action: Partially Implemented

Observations/Findings: District officials told us they began evaluating existing network user accounts each year. In March 2024, District officials performed their first documented review to identify and disable unnecessary network user accounts. However, the District’s review process was not effective in ensuring unnecessary network user accounts were always disabled in a timely manner.

We reviewed documentation of the District's 2024 and 2025 network user account evaluations and noted the following:

- Of the 65 enabled network user accounts identified to be disabled during the District's 2024 review:
    - The unneeded accounts were not always identified and disabled in a timely manner. The identified user accounts were not used to logon to the District's network for an average of 1.5 years and up to 3.6 years prior to being identified as unneeded.
    - Three user accounts were enabled as of May 2025. While two of the user accounts were for employees who were subsequently rehired and authorized for network access, District officials could not provide the business need for the remaining enabled user account.
- Of the 22 enabled network user accounts identified to be disabled during the District's 2025 review:
    - While all 22 user accounts were disabled as of May 2025, the unneeded accounts were not always identified and disabled in a timely manner. The identified user accounts were not used to logon to the District's network for an average of 1.3 years and up to 3.9 years prior to being identified as unneeded. District officials could not provide an explanation for why the accounts not used for multiple years were not identified as unnecessary and disabled during the 2024 review.

District officials could have made their review process more effective by performing the reviews more frequently and/or at times of the year when the District commonly experienced employee turnover, such as after the end of the school year. Without an effective process to evaluate and disable network user accounts, District officials cannot be assured that unnecessary network user accounts will be disabled in a timely manner. Unnecessary network user accounts that remain enabled increase opportunities for users to make unauthorized or improper changes, improperly access students' private and personal information and/or modify records to conceal malicious activity.

Recommendation 4 – Disable Former Employees' Network User Accounts

Disable network user accounts for former employees as soon as these users leave the District.

Status of Corrective Action: Partially Implemented

Observations/Findings: We reviewed all enabled network user accounts assigned to the 54 employees who separated from the District between January 2023 and May 2025. Our review determined the following:

- One user account (2 percent) was disabled in a timely manner.
- As noted in Recommendation 2, one user account (2 percent) was enabled as of May 2025, despite the employee separating from the District in February 2025.
- An additional 19 user accounts (35 percent) were not disabled in a timely manner. On average, these employees left eight months and up to 1.2 years before their accounts were disabled.

- District officials did not document when the remaining 33 user accounts (61 percent) were disabled and, as such, we were unable to determine whether they were disabled in a timely manner.

Not disabling former employees' network user accounts in a timely manner increases the 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 5 – Review Application User Accounts and Limit User Permissions

Review student information and financial application user accounts and limit user permissions based on an individual's job duties and to properly segregate duties.

Status of Corrective Action: Not Implemented

Observations/Findings: District officials told us that they informally discussed the unnecessary and improperly segregated application user accounts and permissions in the financial application identified during our 2022 audit. However, they had not comprehensively reviewed the financial application user accounts and permissions since our audit. We reviewed the user accounts and permissions in the financial application as of May 2025 and determined that District officials had not further segregated user permissions nor had they implemented additional or enhanced compensating controls to further mitigate the risk introduced by the improperly segregated permissions.

District officials also told us that they had not reviewed or further limited student information application user accounts and permissions since our audit. We reviewed the user accounts and permissions in this application as of May 2025 and noted that all five user accounts identified with unnecessary permissions during our audit had not had unnecessary permission removed. Rather, two of the five user accounts (40 percent) were granted additional permissions.

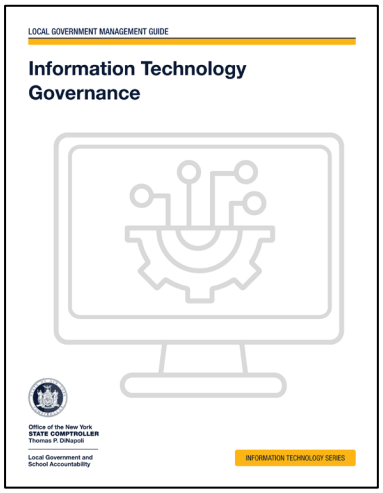
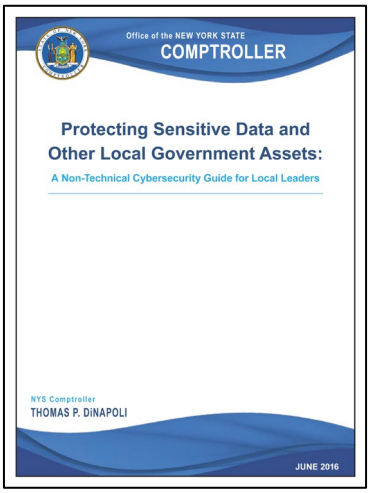
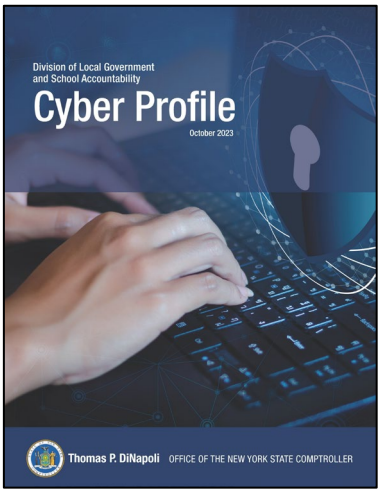
While District officials stated they intended to perform a review of user permissions in the student information application, this review had not occurred as of May 2025 due to other higher-priority matters. District officials did not elaborate on what those higher-priority matters were.

Without limiting and properly segregating application user accounts and permissions, increased opportunities remain for users to make unauthorized or improper changes, improperly access students' private and personal information and/or modify accounting records to conceal malicious transactions.

During our review, we discussed the basis for our recommendations and the operational considerations relating to these issues with District officials. We encourage the Board, officials and IT Managers to continue their efforts to fully implement our recommended improvements. For additional guidance, the Board, officials and IT Managers should refer to the 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*
		
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