DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2020M-82

Naples Central School District

Network Access Controls

OCTOBER 2020

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

Contents

Report Highlights

Naples Central School District

Audit Objective

Determine whether Naples Central School District (District) officials ensured network access controls were secure.

Key Findings

District officials did not ensure that the District's network access controls were secure.

- Officials did not regularly review network user accounts and permissions to determine whether they were appropriate or needed to be disabled.
- The District had 63 unneeded network user accounts that had not been used in at least six months.

In addition, sensitive information technology (IT) control weaknesses were communicated confidentially to officials.

Key Recommendations

- Regularly review network user accounts and disable those that are unnecessary.
- Ensure all IT users have and use their own network user accounts to access the District's network.

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

Background

The District serves residents in the Towns of Bristol, Canadice, Canandaigua, Naples, Richmond and South Bristol in Ontario County; the Towns of Cohocton and Prattsburgh in Steuben County; the Towns of Italy and Middlesex in Yates County; and the Town of Springwater in Livingston County.

The nine-member Board of Education (Board) is responsible for managing and controlling the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the District's chief executive officer and is responsible for the District's administration.

District officials and staff rely on the District's IT assets for Internet access, email and maintaining confidential and sensitive financial and personnel records. The District's IT Director is responsible for monitoring network user accounts and permissions.

Quick Facts

Enabled Network User Accounts	1,047
Student Network User Accounts	742
Nonstudent Network User Accounts	305

Audit Period

July 1, 2018 – May 1, 2020

Network Access Controls

Why Should Officials Monitor Network User Accounts and Permissions?

District officials are responsible for restricting network user access to only those applications, resources and data needed for learning and to complete job duties and responsibilities. This helps ensure data and IT assets are protected from unauthorized use and/or modification.

Network user accounts enable networks, computers and applications to recognize specific users, grant appropriate user permissions and provide user accountability by affiliating network user accounts with specific users. Network user accounts are potential entry points for attackers because, if compromised, they could be used to access and view data stored on the network. When multiple users are allowed to share network user accounts, the District has an increased risk that personal, private and sensitive information (PPSI)[1] could be intentionally or unintentionally changed and/or compromised by unauthorized individuals.

To minimize the risk of unauthorized access, officials should actively manage user accounts and permissions, including their creation, use and dormancy, and regularly monitor them to ensure they are appropriate and authorized. When user accounts are no longer needed, they should be disabled in a timely manner. The District should have written procedures for granting, changing and removing user access and permissions to the overall networked computer system.

When user accounts are no longer needed, they should be disabled in a timely manner.

Generally, administrative accounts have oversight and control of networks, computers and applications with the ability to add new users and change users' passwords and permissions. A user with administrative permissions can make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes.

Additionally, any program that a user with network or local administrative permissions runs will inherently run with the same permissions. For example, if malicious software (malware) installed itself on a computer, it would run at a higher privilege under a user account with administrative permissions, which could result in a greater risk of network or computer compromise and/or data loss. Officials must limit administrative permissions to those users who need them to complete their job functions.

[1] 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.

Officials Did Not Adequately Manage Network User Accounts and Permissions

Unneeded Network User Accounts – The District's data network and security access policy addressed granting, changing and terminating user access to its network based on users' job duties. In November 2019, District officials developed new procedures, which included maintaining written checklists and a spreadsheet, to help ensure access is granted and revoked as needed.

During our review of all 305 nonstudent network user accounts, we found that 89 user accounts (29 percent) had not been used in at least six months. Also, seven of the 89 accounts had never been used. Of the 89 accounts, the IT Director told us 63 were unneeded, should have been disabled and that she would disable them.

Before November 2019, the District did not have an effective process in place to periodically review user accounts. As a result, officials were unaware that these 63 unneeded user accounts were still enabled.

Unneeded Generic[2] and/or Shared Accounts – During our review of 63 unneeded network user accounts, we found that 29 accounts were generic and/or shared accounts.[3] The IT Director identified an additional nine generic and/or shared accounts that were used in the last six months but were no longer needed. The Director told us she would disable the additional nine accounts.[4]

Unneeded network user accounts can be potential entry points for attackers because they are not monitored or used and, if accessed by an attacker, possibly could be used to inappropriately access and view PPSI. Also, when a District has many user accounts that must be managed and reviewed, unneeded user accounts may make it more difficult to manage network access. In addition, if users share accounts, accountability is diminished and activity in the system may not be able to be traced back to a single user.

Unnecessary Administrative Permissions – During our review of all 305 nonstudent network user accounts, we found that 20 user accounts had administrative permissions. According to the IT Director, five of these accounts were unneeded and that she would disable them.

When users have unneeded administrative permissions to networks and computers they could make unauthorized changes that might not be detected.

When users have unneeded administrative permissions to networks and computers they could make unauthorized changes that might not be detected.

[2] Generic accounts are used by certain network services to run properly and can be created for services that are not linked to a personal account to meet various business needs.

[3] The shared accounts were being shared among various users.

[4] The 29 accounts were included in the 63 unneeded network user accounts that the IT Director told us she would disable. Refer to the Unneeded Network User Accounts section for further information.

In addition, the misuse of administrative permissions is a method often used by attackers to compromise or disrupt systems.

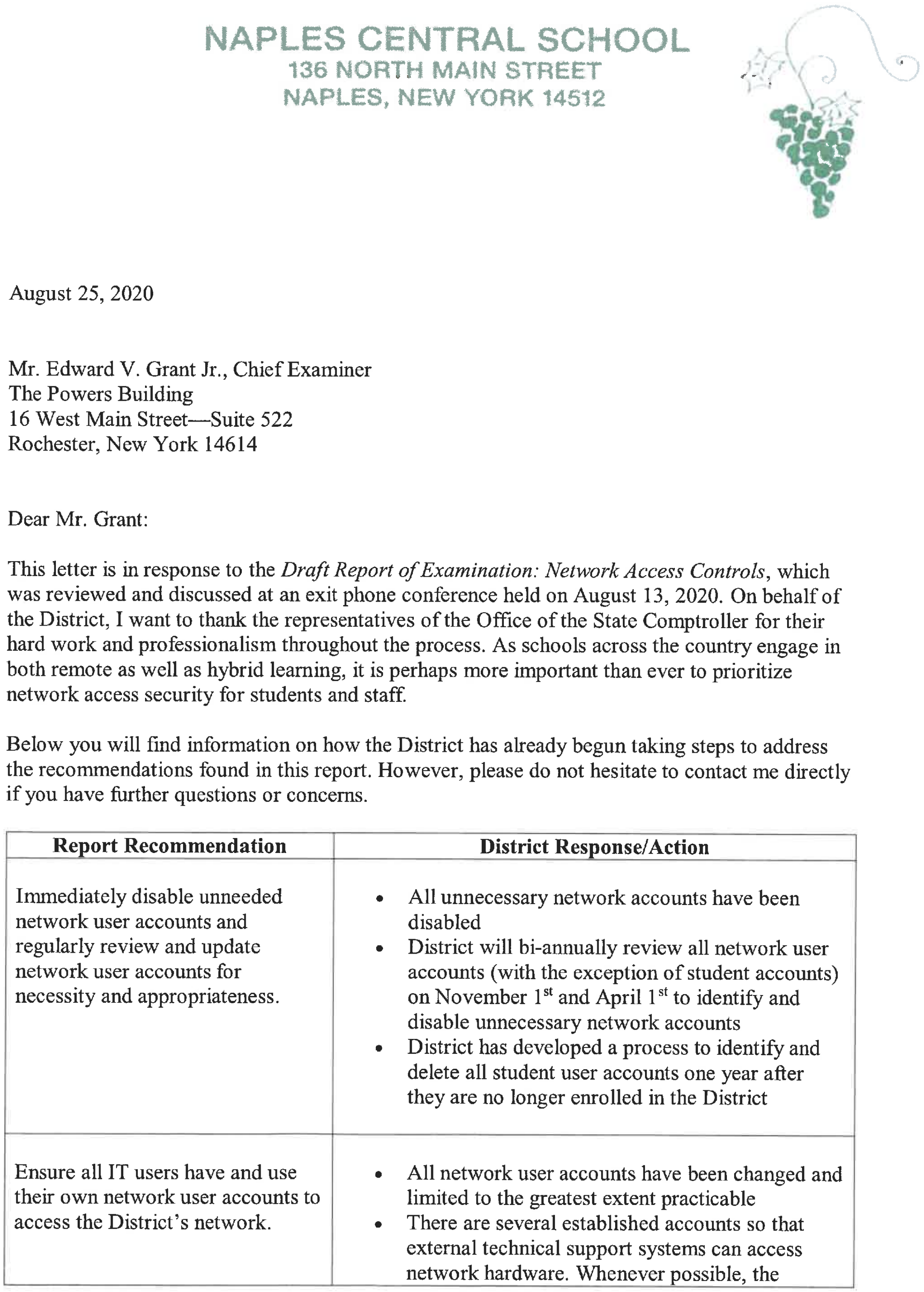
A user can be deceived into opening a malicious email attachment, downloading and opening a file from a malicious website, or accessing a website programmed to automatically infect the user's computer with malicious software. If the deceived user has administrative permissions, an attacker could use those elevated privileges to cause greater damage than with a lesser-privileged account.

What Do We Recommend?

District officials should:

1. Immediately disable unneeded network user accounts and regularly review and update network user accounts for necessity and appropriateness.
2. Ensure all IT users have and use their own network user accounts to access the District's network.
3. Assess network user permissions on a regular basis and remove excessive user permissions for those users who do not need that level of access to perform their current job duties.

Appendix A: Response From District Officials



NAPLES CENTRAL SCHOOL
136 NORTH MAIN STREET
NAPLES, NEW YORK 14512

August 25, 2020

Mr. Edward V. Grant Jr., Chief Examiner
The Powers Building
16 West Main Street—Suite 522
Rochester, New York 14614

Dear Mr. Grant:

This letter is in response to the *Draft Report of Examination: Network Access Controls*, which was reviewed and discussed at an exit phone conference held on August 13, 2020. On behalf of the District, I want to thank the representatives of the Office of the State Comptroller for their hard work and professionalism throughout the process. As schools across the country engage in both remote as well as hybrid learning, it is perhaps more important than ever to prioritize network access security for students and staff.

Below you will find information on how the District has already begun taking steps to address the recommendations found in this report. However, please do not hesitate to contact me directly if you have further questions or concerns.

Report Recommendation	District Response/Action
Immediately disable unneeded network user accounts and regularly review and update network user accounts for necessity and appropriateness.	• All unnecessary network accounts have been disabled • District will bi-annually review all network user accounts (with the exception of student accounts) on November 1st and April 1st to identify and disable unnecessary network accounts • District has developed a process to identify and delete all student user accounts one year after they are no longer enrolled in the District
Ensure all IT users have and use their own network user accounts to access the District's network.	• All network user accounts have been changed and limited to the greatest extent practicable • There are several established accounts so that external technical support systems can access network hardware. Whenever possible, the

	account names have been changed so that they do not reflect generic or high level access. This will be the standard operating procedure moving forward
Assess network user permissions on a regular basis and remove excessive user permissions for those users who do not need that level of access to perform their current job duties.	• District will conduct a review of all network user accounts (with the exception of student accounts) bi-annually on November 1st and April 1st to determine the appropriate levels of access needed by individuals to conduct their current work responsibilities

Again, the District would like to thank the representatives of the Office of the State Comptroller for their insight and assistance. We are fortunate to have a faculty and staff committed to ensuring that the Naples Central School District remains a safe place to teach and learn, and we will use the recommendations to enhance our current practices, policies, and procedures.

Sincerely,

Matthew Frahm, Ed.D.
Superintendent of Schools

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 reviewed the District's IT policies and procedures and interviewed District officials to gain an understanding of IT operations, specifically those related to the granting, modification and revocation of network user accounts and permissions.
- We examined network user account and security settings using specialized audit software. We reviewed the network user and administrator accounts and compared them to current employee lists to identify inactive and possibly unneeded network user accounts. We reviewed automated settings to identify any settings that indicated ineffective IT controls.
- We followed-up with District officials on possibly unneeded accounts and automated settings that indicated ineffective IT controls.

Our audit also examined the adequacy of certain IT 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.

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

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner

The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608

Tel (585) 454-2460 • Fax (585) 454-3545 • Email: Muni-Rochester@osc.ny.gov

Serving: Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

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