DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2021M-35

Phelps-Clifton Springs Central School District

Network Access

JUNE 2021

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

Contents

Report Highlights

Phelps-Clifton Springs Central School District

Audit Objective

Determine whether Phelps-Clifton Springs 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. As a result, we identified 139 unneeded user accounts, 36 unneeded generic or shared user accounts and five user accounts with unnecessary administrator permissions.
- Maintain hardware or software inventory records.

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.
- Maintain detailed, up-to-date inventory records for all computer hardware and software.

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

Background

The District serves the Towns of Hopewell, Manchester, Phelps, and Seneca in Ontario County, the Town of Junius in Seneca County and the Towns of Arcadia and Lyons in Wayne County.

The District is governed by a seven-member Board of Education (Board) responsible for managing and controlling financial and educational affairs.

The Superintendent of Schools is the chief executive officer and responsible for District administration.

The District's Director of Technology (IT Director) is responsible for monitoring network user accounts and permissions.

The District relies on its IT assets for Internet access, email and maintenance of financial, personnel and student records.

Quick Facts

Network User Accounts	
Students	1,577
Nonstudents	803
Computer Devices (Laptops and Tablets)	2,390

Audit Period

July 1, 2018 – February 18, 2021

Network Access

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 provide users with access to network resources and should be actively managed to minimize risk of misuse. If not properly managed, network user accounts could be potential entry points for attackers because they could be used to inappropriately access and view personal, private and sensitive information (PPSI),[1] make changes to the records or deny access to electronic information.

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. A district should have written procedures for granting, changing, disabling and removing user access and permissions to the network.

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

Generally, an administrative account has permissions to monitor and control a network, computers and applications that can include adding new users and changing user 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. As a result, officials must limit administrative permissions to those users who need them to complete their job functions.

Additionally, any program that a user with 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.

[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

District officials configured specialized software to automatically manage user accounts on the network. However, they did not establish policies or procedures to add, disable or change user permissions. As a result, the District had unneeded, unused and shared network user accounts and permissions that were not disabled or monitored. We reviewed all 2,380 enabled network user accounts for IT security weaknesses.

Unneeded Network User Accounts – We found 478 user accounts (437 nonstudent accounts and 41 student accounts) had not been used in at least six months. The IT Director said 328 of these accounts were for the Wayne-Finger Lakes Board of Cooperative Educational Services (BOCES) staff to access the BOCES-leased classrooms in the buildings using electronic key fobs.

However, we determined that 83 of the 328 BOCES accounts were unnecessary because the user was no longer employed by BOCES. The IT Director said that he would disable these accounts after he confirmed their status with BOCES.

The IT Director also told us he disabled 56 of the remaining 150 user accounts because they were unneeded and that the remaining 339 user accounts were necessary.

Unneeded Generic or Shared Accounts – 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. A shared network user account is an account with a username and password that is shared among two or more people. Shared accounts are often used to provide access to guests and temporary or intermittent IT users (e.g., substitute teachers and third-party vendors) and automated processes (e.g., backups and testing).

We found 95 generic or shared network user accounts, of which 72 were not used in the last six months. The IT Director told us that he reviewed these accounts and disabled 36 unnecessary accounts.

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. When the 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, because employees shared user accounts, accountability was diminished and activity in the system could not be traced back to a specific user.

Unnecessary Administrative Permissions – We found that five of the 24 accounts with administrative permissions were unnecessary. The IT Director told us that he disabled these five user accounts because they did not require these permissions.

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

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

Why Should Officials Maintain Hardware and Software Inventories?

Computer equipment and software management is essential to safeguarding district IT assets, PPSI and data. Officials should maintain detailed, up-to-date inventory records of all computer hardware devices and software to safeguard IT assets. Reliable IT inventory records are critical for protecting these assets from loss or misuse.

District officials cannot properly track and protect IT assets if they do not know what IT assets they have and where those assets reside. The failure to maintain detailed, up-to-date inventory exposes these valuable assets to an increased risk of loss, theft or misuse, putting district data and PPSI at risk.

Information maintained for each piece of computer equipment should include a description of the item, name of the employee to whom the equipment is assigned, physical location of the equipment and relevant purchase or lease information. Officials should verify the accuracy of inventory records through periodic physical inventory counts.

Officials must actively manage all software installed because attackers are always looking for vulnerable versions of software than can be remotely exploited. Without proper knowledge or control of the software deployed in an organization, officials cannot properly secure their IT assets.

Poorly controlled devices are more likely to be either running software that is unneeded for business purposes (introducing potential security flaws), or running malware introduced by an attacker after a system is compromised. Organizations that do not have complete software inventories are unable to find systems running vulnerable or malicious software to mitigate problems or root out attackers.

Managed control of all hardware and software also plays a critical role in planning and executing system backup, incident response, and recovery.

Officials Did Not Provide Hardware and Software Inventory Records

Although the IT Director provided us with the approximate number of devices that connect to the District's network, officials did not provide us with formal hardware and software inventory records he purported to maintain. The absence of complete, accurate or reliable IT inventory records puts the District's IT assets at an increased risk of loss, theft, or misuse.

Without proper identification of all devices on a network, unauthorized devices and software could be easily introduced, putting organizational data at risk. Furthermore, without adequate inventory records, District officials cannot ensure effective patch management and software licensing compliance. Poor records make it unlikely that software patches necessary to address known security vulnerabilities are applied on a timely basis, if at all.

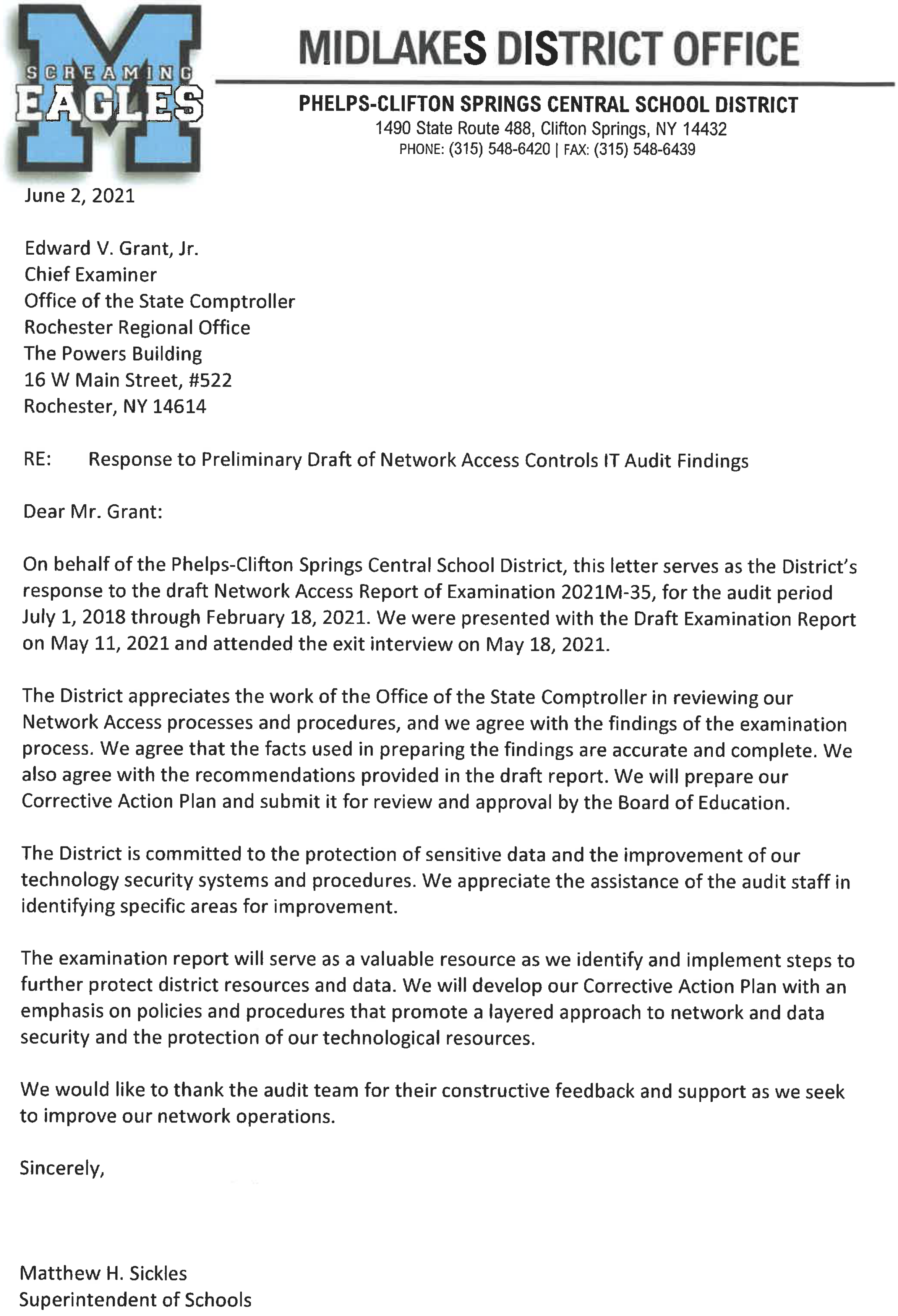
In addition, insufficient software inventory records increase the likelihood of inadvertently violating copyright laws by having more software users than licenses for a particular application, which could result in the District incurring significant software infringement penalties.

What Do We Recommend?

District officials should:

1. Regularly review and update network user accounts for necessity and appropriateness.
2. Ensure all IT users have and use their own unique network user accounts. Routinely evaluate shared user accounts and disable those that are no longer needed.
3. Assess network user permissions on a regular basis and ensure that network user accounts provide users with appropriate permissions needed to perform their job duties.
4. Maintain detailed, up-to-date IT hardware and software inventory records.

Appendix A: Response From District Officials



MIDLAKES DISTRICT OFFICE

PHELPS-CLIFTON SPRINGS CENTRAL SCHOOL DISTRICT
1490 State Route 488, Clifton Springs, NY 14432
PHONE: (315) 548-6420 | FAX: (315) 548-6439

June 2, 2021

Edward V. Grant, Jr.
Chief Examiner
Office of the State Comptroller
Rochester Regional Office
The Powers Building
16 W Main Street, #522
Rochester, NY 14614

RE: Response to Preliminary Draft of Network Access Controls IT Audit Findings

Dear Mr. Grant:

On behalf of the Phelps-Clifton Springs Central School District, this letter serves as the District's response to the draft Network Access Report of Examination 2021M-35, for the audit period July 1, 2018 through February 18, 2021. We were presented with the Draft Examination Report on May 11, 2021 and attended the exit interview on May 18, 2021.

The District appreciates the work of the Office of the State Comptroller in reviewing our Network Access processes and procedures, and we agree with the findings of the examination process. We agree that the facts used in preparing the findings are accurate and complete. We also agree with the recommendations provided in the draft report. We will prepare our Corrective Action Plan and submit it for review and approval by the Board of Education.

The District is committed to the protection of sensitive data and the improvement of our technology security systems and procedures. We appreciate the assistance of the audit staff in identifying specific areas for improvement.

The examination report will serve as a valuable resource as we identify and implement steps to further protect district resources and data. We will develop our Corrective Action Plan with an emphasis on policies and procedures that promote a layered approach to network and data security and the protection of our technological resources.

We would like to thank the audit team for their constructive feedback and support as we seek to improve our network operations.

Sincerely,

Matthew H. Sickles
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 granting, modifying and disabling network user accounts and permissions.
- We examined network user account and security settings using a specialized audit script. 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 potentially unneeded accounts and automated settings that indicated ineffective controls.

Our audit also examined the adequacy of certain information technology 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
https://www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
https://www.osc.state.ny.us/local-government/publications

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
https://www.osc.state.ny.us/local-government/publications

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
https://www.osc.state.ny.us/files/local-government/publications/pdf/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
https://www.osc.state.ny.us/local-government/publications

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