DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2020M-122

Clyde-Savannah Central School District

Network Access Controls

JANUARY 2021

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Clyde-Savannah Central School District

Audit Objective

Determine whether Clyde-Savannah 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 the following unneeded accounts:
  - 354 network user accounts (33 percent)
  - 53 generic and/or shared user accounts (53 percent)
  - Five administrative user accounts (19 percent)

In addition, sensitive information technology (IT) control weaknesses were communicated confidentially to officials. Due to the COVID-19 pandemic, as the District moves to increased reliance on a remote learning environment and administrative operations, protecting IT assets becomes more critical.

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 indicated they planned to initiate corrective action.

Background

The District serves the Towns of Butler, Galen, Lyons, Rose and Savannah in Wayne County and the Towns of Junius and Tyre in Seneca County. The District is governed by a nine-member Board of Education (Board) responsible for managing and controlling the District's financial and educational affairs. The Superintendent of Schools is the chief executive officer and 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, student and personnel records. The District's Director of Instructional Technology, Innovation and Data Privacy Officer (IT Director) is responsible for monitoring network user accounts and permissions. The current IT Director was appointed in July 2020. Before July 2020, the District contracted with the Wayne Finger Lakes Board of Cooperative Educational Services (BOCES) for a shared IT Coordinator to oversee IT operations.

Quick Facts	
Students	977
Nonstudent	448
Total Enabled	1,425

Audit Period

July 1, 2018 – August 6, 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 inappropriately access and view data stored on the network.

Officials should routinely evaluate generic network user accounts and disable those that are not related to a current district or system need.[1] In addition, when multiple users are allowed to share network user accounts, a district has an increased risk that personal, private and sensitive information (PPSI)[2] could be intentionally or unintentionally changed and/or compromised by unauthorized individuals.

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

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

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 network of 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

[1] Generic accounts are used by certain network services to run properly and can be created for services that are not linked to an individual user account. For example, generic accounts can be used for classroom instructional purposes or to scan student tests.

[2] 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.

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 Did Not Adequately Manage Network User Accounts and Permissions

Officials did not adequately manage network user accounts and permissions for the District's network. We examined all network user accounts to determine whether any were unneeded or had unneeded administrative permissions.

Unneeded Network User Accounts – The District established procedures to add, disable and change user permissions, which included the completion of a standard form to help ensure network access was granted and disabled as needed. However, IT staff told us that while staff were generally diligent about completing this form to add or change user permissions, staff did not consistently complete the form when permissions needed to be disabled.

During our review, we identified 883 user accounts (62 percent) that had not been used in at least six months.[3] We found 224 accounts (25 percent) belonged to senior class students, who had already graduated and should have been disabled and/or deleted. The IT Director said that the amount of unneeded accounts was likely higher because users were working remotely due to the pandemic, and many were not logging into the network. The IT Director told us that IT staff reviewed all the network user accounts we identified and confirmed that those determined to be unnecessary were deleted or disabled.

The IT Director said that the IT staff deleted or disabled 354 of the enabled accounts we questioned the need for. Therefore, a total of 1,071 enabled accounts remained (796 student and 275 nonstudent). Further, the District was also able to delete an additional 962 accounts, which were already disabled, but determined to be unnecessary. These accounts primarily belonged to students who had graduated.

Unneeded Generic and/or Shared Accounts – During our review of all enabled network user accounts, we identified 100 generic and or/shared network user accounts (7 percent) shared among various users. The IT Director told us that IT staff reviewed these accounts and disabled or deleted 53 accounts (53 percent) that were unnecessary. We determined that the 47 remaining accounts (47 percent) were appropriate because they were used by BOCES staff for specifically identified purposes, or by IT staff for maintenance.

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

[3] 666 student accounts and 217 non-student accounts

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, 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 – During our review of all enabled network user accounts, we found 26 accounts with administrative permissions. The IT Director told us that IT staff disabled administrative permissions for five of these accounts (19 percent) that did not require these permissions. The remaining accounts were for IT purposes, and required to administer the system.

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.

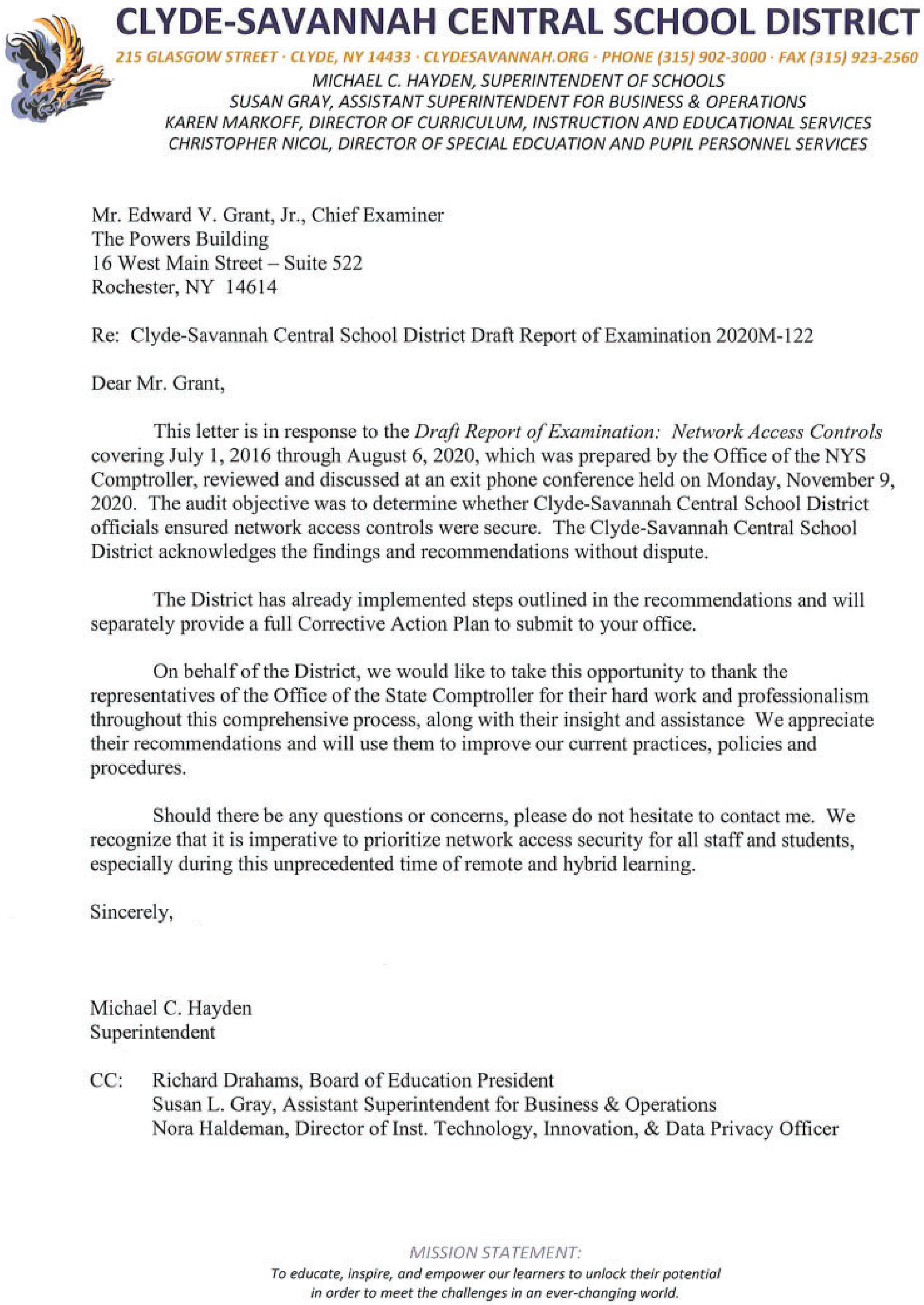
When users have unneeded administrative permissions to networks and computers, they could make unauthorized changes that might not be detected.

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 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



CLYDE-SAVANNAH CENTRAL SCHOOL DISTRICT

215 GLASGOW STREET · CLYDE, NY 14433 · CLYDESAVANNAH.ORG · PHONE (315) 902-3000 · FAX (315) 923-2560

MICHAEL C. HAYDEN, SUPERINTENDENT OF SCHOOLS
SUSAN GRAY, ASSISTANT SUPERINTENDENT FOR BUSINESS & OPERATIONS
KAREN MARKOFF, DIRECTOR OF CURRICULUM, INSTRUCTION AND EDUCATIONAL SERVICES
CHRISTOPHER NICOL, DIRECTOR OF SPECIAL EDCUATION AND PUPIL PERSONNEL SERVICES

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

Re: Clyde-Savannah Central School District Draft Report of Examination 2020M-122

Dear Mr. Grant,

This letter is in response to the *Draft Report of Examination: Network Access Controls* covering July 1, 2016 through August 6, 2020, which was prepared by the Office of the NYS Comptroller, reviewed and discussed at an exit phone conference held on Monday, November 9, 2020. The audit objective was to determine whether Clyde-Savannah Central School District officials ensured network access controls were secure. The Clyde-Savannah Central School District acknowledges the findings and recommendations without dispute.

The District has already implemented steps outlined in the recommendations and will separately provide a full Corrective Action Plan to submit to your office.

On behalf of the District, we would like to take this opportunity to thank the representatives of the Office of the State Comptroller for their hard work and professionalism throughout this comprehensive process, along with their insight and assistance We appreciate their recommendations and will use them to improve our current practices, policies and procedures.

Should there be any questions or concerns, please do not hesitate to contact me. We recognize that it is imperative to prioritize network access security for all staff and students, especially during this unprecedented time of remote and hybrid learning.

Sincerely,

Michael C. Hayden
Superintendent

CC: Richard Drahams, Board of Education President
Susan L. Gray, Assistant Superintendent for Business & Operations
Nora Haldeman, Director of Inst. Technology, Innovation, & Data Privacy Officer

MISSION STATEMENT:
To educate, inspire, and empower our learners to unlock their potential
in order to meet the challenges in an ever-changing world.

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 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 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
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