DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2022M-77

Nassau Board of Cooperative Educational Services

Network User Account Controls

SEPTEMBER 2022

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

Contents

Report Highlights

Nassau Board of Cooperative Educational Services

Audit Objective

Determine whether Nassau Board of Cooperative Educational Services (BOCES) officials established adequate controls over non-student network user accounts to help prevent unauthorized use, access and/or loss.

Key Findings

BOCES officials did not establish adequate controls over network user accounts. As a result, BOCES has an increased risk of unauthorized access to and use of the BOCES network and potential loss of important data. In addition to sensitive information technology (IT) control weaknesses that were confidentially communicated to officials, we found BOCES officials did not:

- Disable 73 unnecessary individual non-student network user accounts and three service accounts with administrative rights.
- Establish written procedures for granting, verifying, changing and disabling network user account access.

Key Recommendations

- Evaluate all non-student network user accounts and ensure unneeded user accounts are disabled in a timely manner.
- Establish written procedures for granting, verifying, changing and disabling non-student network user account access.
- Establish and implement a system in which non-employee network user accounts and service accounts are disabled after a specified period without a valid user login.

BOCES officials generally agreed with our findings and indicated they plan to initiate corrective action.

Background

BOCES is composed of 56 component school districts in Nassau County and is governed by a nine-member Board of Education (Board), with members elected by Boards of Education of the component districts. The Board is responsible for the general management and oversight of BOCES' financial and educational affairs. The District Superintendent (Superintendent) is the chief executive officer and is responsible, along with other administrative staff, for the day-to-day management under the Board's direction.

The Associate Director of Technology Services (Director) is responsible for establishing controls over BOCES' network user accounts. BOCES Technology Services Department (Department) staff, including the Executive Manager, monitor and service the network under the supervision of the Director.

Quick Facts	
Employees	6,101
Students Served	28,204
Enabled Non-Student Network User Accounts	8,962

Audit Period

July 1, 2020 – September 29, 2021

Network User Account Controls

How Should Officials Establish Controls Over Network User Accounts?

Network user accounts provide access to network resources and should be actively managed to minimize the risk of unauthorized use, access and loss. A network administrative account has elevated permissions to monitor and control a network, connected computers and certain applications with the ability to add new users and change users' passwords and permissions. 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 records or deny legitimate access to electronic information.

To minimize the risk of unauthorized use, access and loss, BOCES officials should actively manage network user accounts, including their creation, use and dormancy, and regularly monitor them to ensure they are appropriate and authorized. When network user accounts, especially network administrative accounts, are no longer needed, they should be disabled in a timely manner. One way to accomplish this is to establish and implement a system in which user accounts are disabled after a reasonable specified period without a valid user login. Officials should regularly review enabled network user accounts to ensure they are still needed and disable unnecessary or unneeded accounts when they are no longer needed.

BOCES officials did not establish adequate controls over network user accounts for the BOCES' network.

Officials Did Not Establish Adequate Controls Over Network User Accounts

BOCES officials did not establish adequate controls over network user accounts for the BOCES' network. They did not establish written procedures for granting, verifying, changing and disabling network user account access.

BOCES uses software to help automate the process of creating and disabling individual non-student network user accounts. On a nightly basis, the software application automatically scans for changes to personnel accounts and automatically creates a new network user account for any new employee and disables the existing network user account of any terminated employee. However, BOCES officials do not periodically review user access and disable user accounts when network access is no longer needed.

BOCES does not use the automated process for creating network accounts for third-party users, such as consultants. To create a third-party network account, the BOCES department requesting a third-party network account submits a ticket

[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, students, third parties or other individuals or entities.

to the Department help desk. The requesting BOCES department head also submits a written request to the Director with a reason for the third-party network account and time the third-party needs the network account. Once the Director reviews and approves the third-party network account, an administrator manually creates a network account for the third-party with an appropriate level of access.

We examined all 8,962 enabled non-student network user accounts to determine whether any were not needed. We found a total of 76 user accounts, including 73 individual non-student network user accounts and three service accounts with administrative rights, that were not needed and should have been disabled.

Based on our review of the 73 unneeded individual non-student network user accounts, 46 were for former substitute teachers and part-time or seasonal employees, and 11 were for former consultants. The Director said the accounts of the former employees and consultants were not disabled because their services may be needed in the future. However, 53 of these user accounts, including 45 former employees and eight former consultants, were never used to access the network after being created, so it is doubtful they may be needed in the future. The oldest former employee account was created in February 2017, and the oldest former consultant account was created in September 2019.

The Director agreed that 19 unneeded accounts should have been disabled, including:

- Seven duplicate accounts,
- Six accounts BOCES had no explanation for,
- A former employee account,
- A former Board member account,
- An employee test account, and
- The three service accounts with administrative rights.

The Department Executive Manager said the test account and three service accounts with administrative rights were not disabled because the Department does not have a system in place to identify and disable unnecessary service accounts. The Director said the other individual user accounts were not disabled because they were created prior to BOCES implementing the automated process of creating and disabling individual non-student network user accounts. BOCES officials do not periodically review a list of network user accounts to determine whether any are unnecessary and should be disabled. Conducting periodic reviews of all network user accounts, including service accounts, to determine whether accounts are necessary would help to identify unnecessary accounts, including those with administrative permissions, and disable them in a timely manner.

The unneeded network user accounts are additional entry points into the BOCES network and, if accessed by an attacker, could be used to inappropriately access the BOCES network to view and/or remove personal information; make unauthorized changes to BOCES records; or deny legitimate access to the BOCES network and records. An attacker could use these additional entry points to severely disrupt BOCES operations by:

- Denying BOCES employees network access to electronic information they need to perform their job duties, such as student medical records or individualized education programs;
- Installing malicious software that could cripple and/or completely shut down the BOCES network by accessing a service account with administrative permissions;
- Obtaining and publicly releasing PPSI, such as employee and student dates of birth, home addresses and social security numbers, that could be used to facilitate identity theft;
- Removing and publicly releasing sensitive information related to BOCES operations, such as personnel action reports and other confidential BOCES Board matters that the Board would discuss during the executive session of a BOCES Board meeting; and
- Inappropriately accessing and changing BOCES records, such as student grades.

Compromising a network user account with administrative permissions could cause greater damage than compromising lesser-privileged accounts because administrative accounts have full control over the network. These events could have criminal, civil, regulatory, financial and reputational impacts on BOCES operations. When an organization has many network user accounts that must be managed and reviewed, unneeded network user accounts increase the risk of inappropriate access by users with malicious intent.

What Do We Recommend?

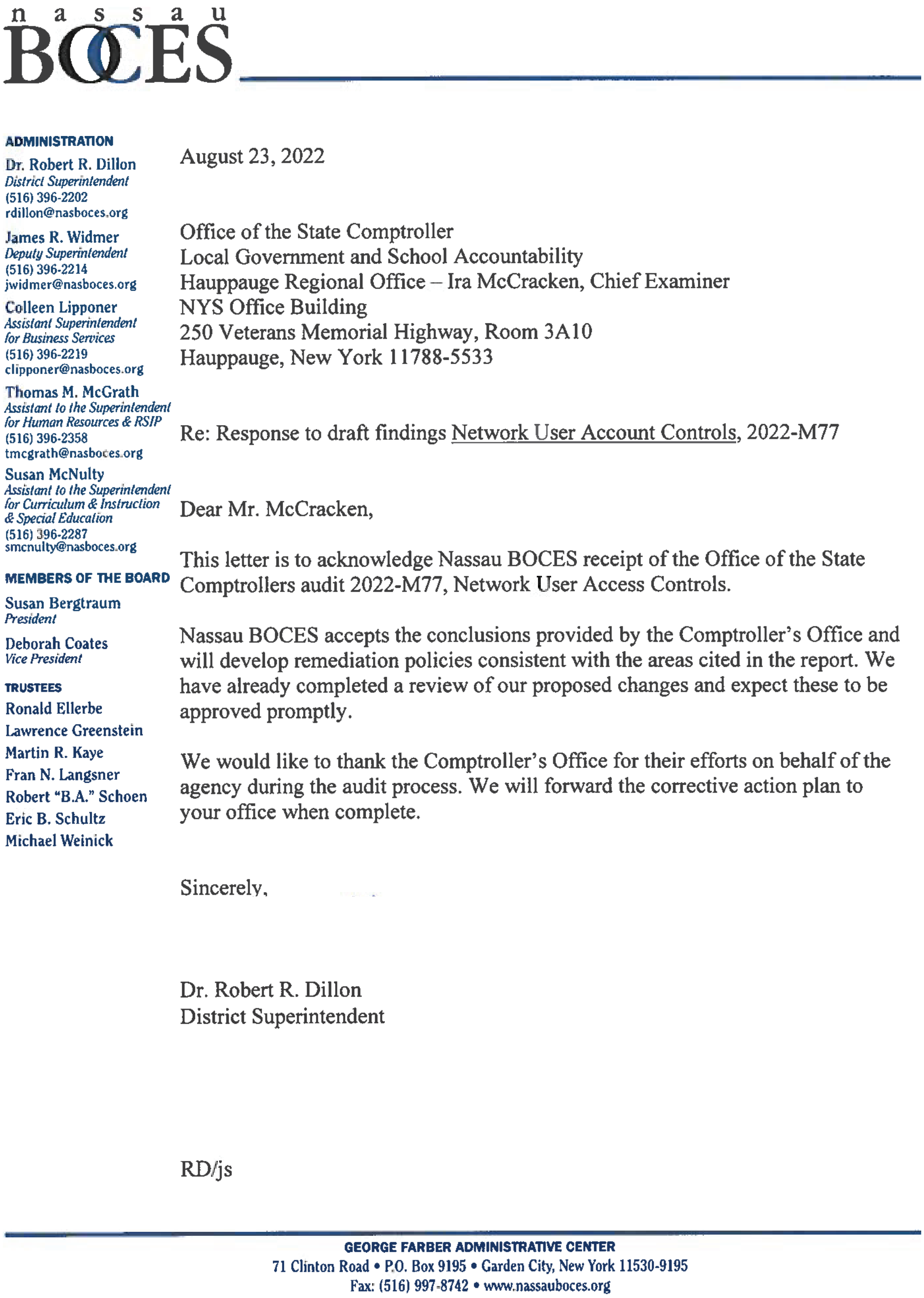
The Director should:

1. Develop and adhere to written procedures for granting, verifying, changing and disabling non-student network user account access.
2. Disable network user accounts of former employees and consultants as soon as they leave BOCES employment or service, and disable any other unneeded user accounts, especially those with administrative rights.

3. Establish and implement a system in which non-employee network user accounts are disabled after a reasonable specified period without a valid user login.

4. Develop a system to periodically review network user accounts to determine whether any are unnecessary and should be disabled.

Appendix A: Response From BOCES Officials



nassau BOCES

ADMINISTRATION

Dr. Robert R. Dillon
District Superintendent
(516) 396-2202
rdillon@nasboces.org

James R. Widmer
Deputy Superintendent
(516) 396-2214
jwidmer@nasboces.org

Colleen Lipponer
Assistant Superintendent for Business Services
(516) 396-2219
clipponer@nasboces.org

Thomas M. McGrath
Assistant to the Superintendent for Human Resources & RSIP
(516) 396-2358
tmcgrath@nasboces.org

Susan McNulty
Assistant to the Superintendent for Curriculum & Instruction & Special Education
(516) 396-2287
smcnulty@nasboces.org

August 23, 2022

Office of the State Comptroller
Local Government and School Accountability
Hauppauge Regional Office – Ira McCracken, Chief Examiner
NYS Office Building
250 Veterans Memorial Highway, Room 3A10
Hauppauge, New York 11788-5533

Re: Response to draft findings Network User Account Controls, 2022-M77

Dear Mr. McCracken,

This letter is to acknowledge Nassau BOCES receipt of the Office of the State Comptrollers audit 2022-M77, Network User Access Controls.

Nassau BOCES accepts the conclusions provided by the Comptroller's Office and will develop remediation policies consistent with the areas cited in the report. We have already completed a review of our proposed changes and expect these to be approved promptly.

We would like to thank the Comptroller's Office for their efforts on behalf of the agency during the audit process. We will forward the corrective action plan to your office when complete.

Sincerely,

Dr. Robert R. Dillon
District Superintendent

RD/js

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 BOCES' IT policies and procedures and interviewed the Director and a Senior Manager II in the Department of Human Resources to gain an understanding of network user account controls, specifically those related to the granting, verifying, changing and disabling of network user account access.
- We examined network user accounts, including their permissions and security settings, using a computerized audit script run on September 29, 2021. We reviewed all enabled non-student network user accounts and compared them to current employee lists to identify inactive and possibly unneeded network user accounts. We reviewed security settings and compared them to current industry standards to identify inconsistencies.
- We followed-up with the Director, an Executive Manager and two Information Technology Specialist II's in the Department of Curriculum, Information and Technology to discuss possible unneeded network user accounts and security settings that were inconsistent with current industry standards.

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 BOCES 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.

Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

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. We encourage the Board to make the CAP available for public review in the District Clerk’s office.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
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
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
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
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

HAUPPAUGE REGIONAL OFFICE – Ira McCracken, Chief Examiner

NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York
11788-5533

Tel (631) 952-6534 • Fax (631) 952-6091 • Email: Muni-Hauppauge@osc.ny.gov

Serving: Nassau, Suffolk counties

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