New York State Comptroller
THOMAS P. DiNAPOLI

Eastern Suffolk Board of Cooperative Educational Services

Information Technology

2023M-93 | October 2023

Division of Local Government and School Accountability

Contents

Report Highlights **1**

Network and Financial Application Access **2**

How Should BOCES Officials Manage Network and Financial Application User Accounts? 2

BOCES Officials Did Not Adequately Manage Network User Accounts 2

What Do We Recommend? 4

Appendix A – Response From BOCES Officials **5**

Appendix B – Audit Methodology and Standards **6**

Appendix C – Resources and Services **7**

Report Highlights

Eastern Suffolk Board of Cooperative Educational Services

Audit Objective

Determine whether Eastern Suffolk Board of Cooperative Educational Services (BOCES) officials managed user account access to the network and financial application.

Key Findings

Although BOCES officials restricted user account access to the financial application, they did not adequately manage user account access to the network. As a result, BOCES had an increased risk that the network could be accessed by unauthorized individuals. In addition to sensitive information technology (IT) control weaknesses that were confidentially communicated to BOCES officials, we found that officials did not:

- Disable 681 network user accounts (18 percent) that were not needed or logged in to for at least six months, including:
  - 165 student accounts,
  - 199 nonstudent accounts, and
  - 317 shared and service accounts.

Key Recommendations

- Periodically review all enabled network user accounts for necessity and disable unnecessary network user accounts in a timely manner.

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

Background

BOCES is an inclusive educational cooperative of 51 Suffolk County school districts, that provides regional leadership and advocacy, direct instruction, management, and support through quality, cost-effective instructional programs, and shared services.

BOCES is governed by a 15-member BOCES Board (Board) elected by the boards of its component districts. The Board is responsible for the general management and oversight of BOCES' financial and educational affairs. The District 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 Office of Technology Integration, overseen by the IT Director and Network Manager, is responsible for setting up user accounts within the financial application and for managing and setting up BOCES' IT network, including securing user account access to the network.

Quick Facts	
Student Enrollment	1,613
Full-Time Teachers	353
Enabled Network User Accounts	
Student	674
Nonstudent	2,633
Other	514
Total	**3,821**

Audit Period

July 1, 2021 – March 27, 2023

Network and Financial Application Access

BOCES relies on its network, financial application and other IT assets for maintaining financial, student and personnel records, and Internet access and email, much of which contain personal, private, and sensitive information (PPSI). PPSI is any information to which unauthorized access, disclosure, modification, destruction use – or disruption of access or use – could have or cause a severe impact on critical functions, employees, students, third parties or other individuals or entities.

A shared user account has a username and password that is shared among two or more people and can be used to, for example, provide access to guests or other temporary or intermittent users. A service account is created for the sole purpose of running a particular network or system service or application (e.g., automated backup systems).

How Should BOCES Officials Manage Network and Financial Application User Accounts?

Actively managing network and financial application user accounts can help minimize the risk of unauthorized use, access and loss. BOCES officials should disable any account that cannot be associated with a current authorized user or BOCES need, and periodically conduct a user account review to identify and disable any accounts that are no longer needed.

Shared and service network user accounts should be limited in use, as they are not linked to one individual and, therefore, may have reduced accountability. BOCES officials may have difficulty managing the accounts and linking any suspicious activity to a specific user. BOCES officials should routinely evaluate the need for these accounts and disable those that are not related to a current BOCES or system need.

BOCES Officials Did Not Adequately Manage Network User Accounts

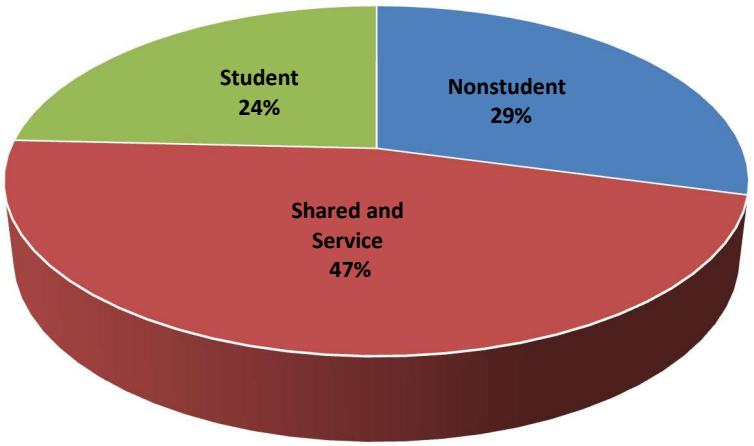
Although the Network Manager adequately restricted financial application user account access to authorized users who required access to conduct their job duties, he did not adequately manage user account access to the network. An authorized user gains access by having a Network User Request form filled out by a supervisor that is signed by an Assistant or Associate Superintendent.

We reviewed all 3,821 enabled network user accounts, including 674 student accounts, 2,633 nonstudent accounts and 514 shared and service accounts. Through consultation with the Network Manager, we determined that 681 network user accounts (18 percent) were not logged in to for at least six months and as much as 17 years and should have been disabled, including 165 student

accounts, 199 nonstudent accounts and 317 shared and service accounts (Figure 1).

FIGURE 1

Unneeded Network User Accounts



Of these 681 accounts, 269 were last logged in to on the date they were created, including 195 user accounts labeled as "necessary" and 41 accounts labeled as "disabled." The Network Manager did not periodically review enabled user accounts to ensure they were necessary and said that reports to review enabled network accounts did not include shared and service user accounts that have not logged in to the network within six months.

As a result of our inquiry, the Network Manager said that BOCES officials updated their process to require reviewing a report of enabled network accounts, including the six-month network user login criteria and disabling accounts that are no longer needed. As of April 25, 2023, the Network Manager stated that they disabled or deleted 149 unnecessary user accounts, including 108 nonstudent accounts and 41 shared accounts.

Unneeded enabled network user accounts are additional entry points into a network and, if accessed by an attacker, could be used to inappropriately access the BOCES network to view and/or remove personal information accessible by that compromised network account; 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:

- Obtaining and publicly releasing PPSI, if it were accessible to a compromised network user account, such as employee and student dates of birth, home addresses and social security numbers − that could be used to facilitate identity theft;

- Denying BOCES employees network access to electronic information they need to perform their job duties, such as student medical records or individual education programs;
- Installing malicious software that could cripple and/or completely shut down BOCES' network by accessing an account with administrative permissions, such as a shared or service account; and
- Removing and publicly releasing sensitive information, if it were accessible to a compromised network user account, related to BOCES operations, such as personnel action reports and other confidential Board matters that the Board would discuss during the executive session of a Board meeting.

What Do We Recommend?

BOCES officials and the Network Manager should:

1. Periodically review all enabled network user accounts for necessity and disable unnecessary network user accounts in a timely manner.

Appendix A: Response From BOCES Officials

Eastern Suffolk BOCES

Educational Services That Transform Lives

David Wicks
District Superintendent/
Chief Executive Officer

October 6, 2023

Mr. Ira McCracken, Chief of Municipal Audits
Division of Local Government and School Accountability
Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788-5533

Dear Mr. McCracken:

First and foremost, the Eastern Suffolk Board of Cooperative Educational Services (Agency) would like to thank the Office of the State Comptroller for their report and recommendations contained therein. The entire process was conducted in a very positive and professional manner, which is a testament to the very insightful, hardworking, and courteous examiners assigned to the engagement. It is our sincere belief that the information obtained from this review will further assist the Agency in its continuous effort to strengthen controls, improve operations, and best protect its technology infrastructure and the sensitive data it stores.

The Agency was provided an opportunity to review the draft report, including the confidential addendum, and meet with the examiners to discuss their findings. We accept and agree with the recommendations and have already implemented remedial measures related to the item in the public report. We respectfully request this also serve as our Corrective Action Plan.

Recommendation: Periodically review all enabled network user accounts for necessity and disable unnecessary network user accounts in a timely manner.

The Office of Technology Integration, in consultation with the Human Resources Department, designed a report to highlight user accounts that have not been active within 180 days. If a user account is inactive for 180 days, it is disabled. In order for the user account to be re-enabled, a new Network User Request form must be submitted and approved. The Office of Technology Integration is also conducting more periodic reviews of non-essential service accounts and those are being disabled and removed, as necessary.

Once again, the Agency expresses its gratitude for the work performed as a part of this examination. We appreciate your assistance and welcome future support.

Should you have any questions or concerns, please do not hesitate to contact us.

Very truly yours,

David Wicks
District Superintendent/
Chief Executive Officer

James J. Stucchio
Associate Superintendent
for Management Services

Middle States Association Commission on Elementary and Secondary Schools — Accredited by MSA CESS

James Hines Administration Center · 201 Sunrise Highway · Patchogue, NY 11772
Phone: (631) 687-3006· Fax: (631) 240-8965 · Email: dwicks@esboces.org
www.esboces.org

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 IT Director (retired in December 2022), Network Manager, Associate Superintendent of Management Services and Director of Business Services to gain an understanding of the IT environment and determine whether officials managed user account access to the BOCES network and financial application.
- We ran a computerized audit script on the BOCES domain controller on January 31, 2023. We analyzed the reports generated by the script and reviewed the last login dates for network user accounts to identify unused and possibly unneeded network user accounts. We compared current employee master list to enabled authorized network users. We followed up with the Network Manager to determine whether the user accounts and financial application access were appropriate and needed.

Our audit also examined the adequacy of certain sensitive 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. The CAP should be posted on BOCES' website for public review.

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 of Municipal Audits

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