New York State Comptroller
THOMAS P. DiNAPOLI

Orange Ulster Board of Cooperative Educational Services

Nonstudent Network User Accounts

2022M-154 | January 2023

Division of Local Government and School Accountability

Contents

Report Highlights

Orange Ulster Board of Cooperative Educational Services

Audit Objective

Determine whether Orange Ulster Board of Cooperative Educational Services (BOCES) officials established adequate internal controls over nonstudent network user accounts to help prevent unauthorized use, access and loss.

Key Findings

BOCES officials did not establish adequate internal controls over network user accounts to help prevent unauthorized use, access and loss. In addition to sensitive information technology (IT) control weaknesses that were communicated confidentially to officials, we found BOCES officials did not:

- Disable 20 unneeded nonstudent network user accounts that had last log-on dates ranging from January 5, 2017 to October 29, 2021.
- Ensure all employees complete IT security awareness training.

Key Recommendations

- Develop written procedures for granting, changing and disabling network user accounts.
- Evaluate all network user accounts and ensure unneeded user accounts are disabled in a timely manner.
- Develop a process to identify and follow up with employees who have not completed the required IT security awareness training.

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

Background

BOCES is composed of 17 component school districts and is governed by a seven-member BOCES Board (Board) elected by the boards 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 the Deputy District Superintendent is the chief operating officer. They are responsible, along with other administrative staff, for the day-to-day management under the Board's direction.

The Deputy District Superintendent is responsible for ensuring IT policies, guidelines and procedures are effectively implemented. The Director of Technology (Director) is responsible for managing BOCES' IT department and operations, including the oversight and management of network user accounts

Quick Facts

Enabled Network User Accounts	
Student	3,099
Nonstudent	1,125
Generic	46
Total	4,270
Enabled Network User Accounts Reviewed	
Nonstudent	1,125
Generic	46
Total	1,171

Audit Period

July 1, 2020 –January 31, 2022. We extended our scope period through May 12, 2022 to complete our IT testing.

Network User Accounts

Why Should Officials Establish Controls Over Network User Accounts?

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. Therefore, BOCES should have written procedures for granting, changing and disabling network user accounts. Network user accounts provide access to network resources and should be actively managed to minimize the risk of unauthorized use, access, or loss. 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. When network user 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.

Officials Did Not Establish Adequate Internal Controls Over Network User Accounts

We reviewed 1,125 enabled nonstudent network user accounts on the BOCES network to determine whether they were necessary and found unnecessary network user accounts were not always disabled in a timely manner.

We found that 20 enabled nonstudent network user accounts were not necessary. Specifically:

- 14 enabled network user accounts were created between October 16, 2015 and March 8, 2022 and assigned to individuals hired by BOCES; however, these individuals never began employment and did not use the accounts to log into the network.
- Six enabled network user accounts were assigned to individuals that are no longer employed by the BOCES and had last log on dates ranging from January 5, 2017 to October 29, 2021.

These unnecessary nonstudent network user accounts have not been disabled and could potentially be used by those individuals or others for malicious purposes.

1 PPSI is any information to which unauthorized access, disclosure modification, destruction – 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.

The Director stated that BOCES relied on a two-step automated review process to manage network accounts. The first step alerted the IT department of any employee that was added, changed positions or was no longer employed by BOCES. The second step involved the new employee logging into the network and changing their password. However, our review determined that the automated review process failed to identify the 20 unnecessary nonstudent network user accounts. The Director indicated that a periodic manual review of all network user accounts would be performed going forward to ensure unnecessary network user accounts are identified and disabled.

Further, BOCES did not have written procedures for granting, changing and disabling network user accounts. The Assistant Director of Technology developed a draft policy including these procedures in January 2022. However, as of January 20, 2023, the draft policy had not been reviewed or adopted by the Board. The Director said user accounts were added when the IT department received an email from human resources when new employees were added to the financial application and disabled when employees were no longer active (e.g., resignation, termination or retirement) and the Board approved the removal of their network user account. In addition, a list of all authorized users was available from the network for BOCES officials to review. However, without written procedures for granting, changing and disabling network user accounts, steps may be missed and the IT department may not be aware of when a network user account should be removed.

Unneeded network user accounts are additional entry points into a network and, if accessed by an attacker, could severely disrupt BOCES operations or 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. 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.

Why Should Officials Provide IT Security Awareness Training?

To minimize the risk of unauthorized access to the network and misuse or loss of data and PPSI, BOCES officials should provide periodic IT security awareness training that explains rules of behavior for using the Internet and IT systems and data and communicate related policies and procedures to all employees and students. The training could center on, but not be limited to, emerging trends such as information theft, social engineering attacks (methods used to deceive users into revealing confidential or sensitive information), computer viruses and other types of malicious software, all of which may result in PPSI compromise or denying authorized network user account access to the IT system and its data.

Training programs should be directed at the specific audience (e.g., system users or administrators).

The training should also cover key security concepts such as the dangers of browsing and downloading files and programs from the Internet; the importance of selecting strong passwords; requirements related to protecting PPSI, and how to respond if an information security or data breach is detected. Additionally, procedures for training should include the review of employees that have not completed the training to ensure 100 percent compliance.

A board and officials should establish a policy and written procedures that require users to be trained in IT security awareness issues and in the usage of the IT infrastructure, software and data. While an IT security awareness policy and procedures will not guarantee the safety of the BOCES' systems, without an adequate policy and procedures to require and provide training that explicitly conveys the appropriate use of a district's computer equipment and practices to safeguard data, officials cannot ensure that employees are aware of their responsibilities.

Officials Did Not Ensure All Network Users Completed IT Security Awareness Training

BOCES officials implemented an online IT security awareness training program for all employees, regardless of their job duties; all BOCES employees have network access. The training included three modules:

- *Reviewing Laws, Regulation, Policies and Procedures,*
- *Understanding, Recognizing and Avoiding Threats,* and
- *Developing Good Habits and Best Practices.*

The training was launched for the 2021-22 fiscal year and was completed by approximately 86 percent of BOCES employees in August, September and October of 2021. However, a report generated by the training program software showed 1,158 network user accounts. Of these 1,158 network user accounts (employee and non-employee), we found 167 nonstudent network account users had not completed the training. BOCES did not have a policy or procedures to ensure all nonstudent network users completed the IT security awareness training.

The Director stated they will be implementing a formal process, in collaboration with the Human Resources department, to identify network account users who have not completed the training and follow up with those employees until the training is completed when they roll out the IT security awareness training for the 2022-23 fiscal year in September 2022. Without ensuring all network users complete periodic, comprehensive IT security awareness training, users may not

understand their responsibilities and are more likely to be unaware of a situation that could compromise BOCES' IT assets and security. As a result, data and PPSI are at a greater risk for unauthorized access, misuse or loss.

What Do We Recommend?

BOCES officials should:

1. Develop and adhere to written procedures for granting, changing and disabling network user account access.

The Director should:

2. Disable network user accounts of former employees as soon as they leave BOCES employment and disable any other unneeded accounts.
3. Develop a system to periodically review network user accounts to determine whether any are unnecessary and should be disabled.
4. Develop a process to identify and follow up with employees that have not completed the required IT security awareness training and consider including those network users that are not employees.

Appendix A: Response From BOCES Officials

January 4, 2023

Office of the State Comptroller
Division of Local Government and School Accountability
Newburgh Regional Office – Dara Disko-McCagg, Chief of Municipal Audits
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725

Re: Response to draft Report of Examination, 2022M-154

Dear Ms. Disko-McCagg,

This letter is to acknowledge Orange-Ulster BOCES receipt of the Office of the State Comptroller's Report of Examination, 2022M-154, Noustudent Network User Accounts.

Orange-Ulster BOCES accepts the conclusions provided by the Comptroller's Office and will develop remediation procedures consistent with the areas noted in the report. As noted in the report, draft procedures were developed and expect these to be approved promptly.

We would like to thank the Comptroller's Office for their efforts on behalf of the organization during the audit process.

Sincerely,

Deborah McBride Heppes
Chief Operating Officer

4 Harriman Drive • Goshen, NY 10924 • (845) 291-0100 • Fax: (845) 291-0129 • www.ouboces.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 Director and Assistant Director to gain an understanding of BOCES' IT environment and internal controls related to network user accounts, and to determine whether IT security awareness training was provided to employees. We reviewed documentation to determine whether network users took and completed the training.
- We examined BOCES' domain controller[2] using a computerized audit script run on March 22, 2022. We analyzed the report by comparing nonstudent network user accounts to a list of current employees to determine whether any network user accounts were no longer necessary. We reviewed the report to determine how long these accounts were inactive.

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 the BOCES's website for public review.

2 The server that controls or manages access to network resources.

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

NEWBURGH REGIONAL OFFICE – Dara Disko-McCagg, Chief of Municipal Audits

33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725

Tel (845) 567-0858 • Fax (845) 567-0080 • Email: Muni-Newburgh@osc.ny.gov

Serving: Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster, Westchester counties