REPORT OF EXAMINATION | 2022M-65

Tompkins-Seneca-Tioga Board of Cooperative Educational Services

Network Access and Information Technology Assets

JULY 2022

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

Contents

Report Highlights

Tompkins-Seneca-Tioga Board of Cooperative Educational Services

Audit Objective

Determine whether Tompkins-Seneca-Tioga Board of Cooperative Educational Services (BOCES) officials ensured network access and information technology (IT) assets were properly safeguarded.

Key Findings

BOCES officials did not ensure network access and IT assets were properly safeguarded from unauthorized use, access and loss. In addition, sensitive IT control weaknesses were communicated confidentially to officials. Officials did not:

- Periodically review and disable unneeded network user accounts resulting in 61 unnecessary accounts.
- Provide adequate IT security awareness training for all employees and contractors.
- Periodically update the IT asset inventory records.

Key Recommendations

- Establish written procedures for adding, modifying, and disabling network user accounts; regularly review existing accounts and disable any unneeded accounts.
- Preserve historical data from IT security awareness training to assess and provide adequate training to users.
- Periodically update the IT asset inventory.

BOCES officials generally agreed with our recommendations and indicated they have initiated corrective action.

Background

BOCES primarily provides educational services to nine component school districts and is governed by a nine-member Board of Education (Board) elected by the boards of the component school districts.

The Board is responsible for the general management and control of financial and educational affairs. The District Superintendent (Superintendent) is the chief executive officer responsible, along with the Assistant Superintendent of Administrative Services (Assistant Superintendent), for the day-to-day management and regional planning and coordination.

The Board designated the Assistant Superintendent as responsible for maintaining the fixed asset inventory, including physical IT assets. The Technology Services Coordinator (Coordinator) reports to the Superintendent and is responsible for all network access management and security, including cybersecurity training.

Quick Facts	
Enabled Network User Accounts	436
Computers/Laptops	470
2021-22 Appropriations	$50.4 million

Audit Period

July 1, 2020 – December 31, 2021. We expanded our audit period through January 31, 2022 to observe software inventory at BOCES facilities.

Network Access and Information Technology Assets

BOCES' network and IT assets are valuable resources. BOCES relies on its network and IT assets for a variety of tasks, many of which substantiate BOCES' day-to-day business functions and operations such as maintaining confidential and sensitive financial and personnel records, Internet access and email. If the network or IT assets are compromised or disrupted, it could cripple BOCES' ability to perform and provide critical services, as well as require extensive effort and resources to evaluate, repair and/or rebuild. While effective network access and IT asset controls do not guarantee their safety, a lack of effective controls significantly increases the risk that the network or IT assets including data, hardware and software systems may be exposed, lost, damaged or held hostage by unauthorized or inappropriate access and use.

BOCES officials are responsible for ensuring that network user accounts are managed appropriately.

How Should BOCES Officials Manage Network User Accounts?

Network user accounts provide access to resources on a BOCES network, as well as connected computers, and should be actively managed to minimize the risk of unauthorized access and misuse. BOCES officials are responsible for ensuring that network user accounts are managed appropriately. If not properly managed, unnecessary network user accounts may not be disabled timely, and they could be additional entry points for attackers to potentially access and view BOCES data inappropriately, make unauthorized changes to records or deny legitimate access to electronic information when needed.

A BOCES should have written procedures for adding, modifying and disabling user account access to the network. Officials should disable unnecessary user accounts as soon as there is no longer a need for them, including user accounts of former employees. In addition, to minimize the risk of unauthorized access, misuse and loss, BOCES officials should regularly review enabled network user accounts to ensure they are still needed.

Generic accounts may be needed for certain network services or applications to run properly but should be limited in use as they are not linked to individual users and therefore may have reduced accountability. For example, generic accounts can be created and used to scan student test scores. Officials should limit the use of generic user accounts and routinely evaluate the need for the accounts and disable those that are not related to a specific academic or system need.

The Coordinator Did Not Establish Procedures to Manage Network User Accounts

The Coordinator did not establish written procedures to add or disable network user accounts or change user account access. For employee network user accounts, the Coordinator used software designed to add new user accounts to the network at employees' start dates and then disable the accounts at their end

dates. For non-employee network user accounts (e.g., third-party contractors and former students), the Coordinator relied on other officials to notify IT staff when an account needed to be added or disabled. Because officials were not periodically reviewing network user accounts, we compared all 436 enabled network user accounts and determined 61 accounts (14 percent) had not been disabled and should have been. Of these 61 accounts, we found:

- 21 unnecessary accounts assigned to third-party contractors and had not been used in at least six months; 16 of which had not been used in more than three years;
- 17 unnecessary generic accounts that were not assigned to an individual or a specific BOCES or system need;
- 16 accounts that belonged to former students or were extraneous student accounts and were not assigned to a student account group;
- Seven accounts belonged to former employees, including former student teachers and interns.

Because the Coordinator relied on automated processes or other staff members to inform them when network user accounts needed to be added or disabled and did not periodically review network user accounts to ensure that their internal processes were functioning correctly, these accounts were not disabled timely and could potentially have been used by former employees, students, contractors or compromised by an attacker to access the network improperly. Therefore, these unnecessary but still enabled user accounts presented an increased risk to the integrity of the network and IT systems.

Why Should BOCES Officials Provide IT and Cybersecurity Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data, and help ensure network access and IT assets are properly safeguarded, BOCES officials should provide periodic IT security awareness training that explains the risks and proper behavior when accessing and using BOCES IT assets and the network. In addition, the training should communicate related policies and procedures to all network users, including contractors.

The training should center on emerging cyber-attack trends such as information theft, social engineering attacks,[1] and computer viruses and other types of malicious software, all of which may result in compromising or denying access to the IT asset used and any data stored on it, or potentially, the entire network.

1 Social engineering attacks are attacks designed to trick a user into providing sensitive data or access to an unauthorized source, such as “phishing”.

BOCES' guidelines require that all staff, as well as contractors, with access to BOCES systems and networks should participate in IT security awareness testing and training. The guidelines provide metrics for measuring passing or failing awareness testing, as well as escalating consequences for repeated failures, such as being assigned different trainings to help target knowledge gaps, meeting with supervisors, meeting with the Coordinator, or potential termination of employment. The Coordinator is responsible for running the IT security awareness and training program and conducting suitable awareness testing to help BOCES' officials ensure network access and IT assets are properly safeguarded.

BOCES' guidelines require that all staff, as well as contractors, with access to BOCES systems and networks should participate in IT security awareness testing and training.

The Coordinator Did Not Adequately Enforce IT and Cybersecurity Awareness Training Requirements

While required by the BOCES' guidelines, contractors who access and use the BOCES network are not receiving any security awareness training. In addition, while current employees were enrolled in a biweekly[2] security awareness test and automatically assigned additional training by the testing program should they fail the test, the Coordinator does not track how often employees fail the test and there are no escalating consequences being enforced. The Coordinator told us employees who fail the test are enrolled in the same training each time they fail a test, which is in violation of the guidelines. The Coordinator stated that it was a time-consuming process to track employees' testing results and escalate the consequences so they stopped doing it.

We reviewed available data from seven security awareness tests conducted by the Coordinator from October 2021 through December 2021 to determine whether employees passed the testing. Of the 280 employees who received security awareness testing during the period, 53 of the 280 employees failed at least once, 12 of the 53 employees failed twice and three of the 12 failed three times.

We were unable to determine whether employees were completing assigned trainings after they failed a security awareness test because the data was not available. The Coordinator was deleting the data after each test to reset for the next test. We discussed with the Coordinator alternative ways to set up each testing cycle to preserve training data. The Coordinator was unable to provide any data confirming that employees were completing required trainings, or that employees who repeatedly failed were properly receiving escalating consequences to address their knowledge gaps, such as alternate trainings on specific topics.

2 Certain employees, based upon job titles, also receive an additional security awareness test on a weekly basis

Because the Coordinator did not provide proper IT security awareness training as mandated by the BOCES security guidelines, employees and contractors at BOCES may not have a proper understanding of the risks from emerging cyber-attacks, and their role as users in helping to ensure network access and IT assets are properly safeguarded. As a result of insufficient training, users could be placing the network and IT assets at an increased risk of unauthorized access and loss of data.

How Should BOCES Officials Monitor and Account for IT Assets?

IT assets can be diverse and represent a significant investment of resources. In addition to servers, user computers, laptops and tablets, IT assets can include monitors, printers, cameras, cellular phones and other hand-held devices. A BOCES board should adopt comprehensive written inventory and disposal policies to help ensure IT assets are properly accounted for, monitored and safeguarded and obsolete or surplus assets are properly disposed of.

BOCES officials should ensure IT assets are protected from loss, inventory records are current, and assets can be easily located. Procedures should include setting dollar value thresholds for identifying and recording assets, tagging assets, and sanitizing assets (such as computers) that may contain sensitive and confidential information before disposal or transfer of the assets.

Officials should also schedule and conduct periodic physical inventories to ensure that all assets listed as being under their control are still located in their proper locations or with the assigned individual. At a minimum, a physical inventory of all IT assets should be conducted annually and any discrepancies between the physical inventory and the digital records should be traced, explained and documented. There should be a process of notification in place when an asset is moved or reassigned.

BOCES' policies and procedures require that all IT assets are inventoried. Officials use inventory management software to maintain and track assets. The software generates a master inventory list of all assets, including IT assets. The list includes the name or description of the asset, its make and model, purchase value, serial number, asset tag number and its assigned location.

The Assistant Superintendent Did Not Properly Monitor and Account for IT Assets

The Assistant Superintendent is responsible for updating and maintaining the master inventory list for all assets, including IT assets. The IT department does not have a process for notifying the Assistant Superintendent if an item is moved or reassigned, and BOCES officials estimated that a physical inventory of assets had not been completed in 10 years.

Because there had not been a physical inventory completed and there was no process in place to record the movement of assets, we attempted to locate 76 IT assets purchased for $166,086 that were listed as active or were physically located at the BOCES main campus to determine whether the inventory list was accurate. These IT assets included older assets that were still listed as active and in service despite having purchase dates of 1997 (eight items), newly purchased assets from the 2020-21 school year (seven items), computers and laptops located in digital media labs (31 items), high-value assets such as servers (three items), and "walkable" assets that were not connected to the network such as televisions, monitors, and digital cameras (27 items).

Of the 76 assets reviewed:

- 36 (47 percent) items purchased for $67,965 were located at the BOCES location stated in the inventory list.
- 16 (21 percent) items purchased for $67,425 were located in a location different than the one stated in the inventory list.
- 24 (32 percent) items purchased for $30,696 were unable to be located by us or BOCES officials. These assets included 12 desktop computers, laptops and tablets purchased for $15,806; seven projectors and monitors purchased for $9,959; two printers purchased for $3,044; and three cameras purchased for $1,887. Officials were unable to provide an explanation for the missing assets.

The Assistant Superintendent told us required annual inventories have not been completed in several years because it was a time-intensive process. However, without written processes for reassigning items, accurate and up-to-date inventory records, and annual inventories, BOCES officials cannot ensure that IT assets are properly safeguarded against theft, loss, or unauthorized access and use.

What Do We Recommend?

The Superintendent should:

1. Ensure the Coordinator implements the recommendations in the public report and confidential IT letter.

The Coordinator should:

2. Establish written procedures for adding, modifying, and disabling network user accounts for all users.
3. Disable unneeded network user accounts as soon as they are no longer needed.

4. Regularly review existing network user accounts for necessity and appropriateness.

5. Preserve historical data from IT security awareness training, use that data to assess and provide adequate training to users, and ensure that the provided training is completed by users.

The Assistant Superintendent should:

6. Have a process in place to be notified when an asset is moved or reassigned, periodically update the IT asset inventory records and annually compare physical IT assets to the digital master list.

Appendix A: Response From BOCES Officials

TST BOCES
TOMPKINS • SENECA • TIOGA

Dr. Jeffrey A. Matteson
District Superintendent and CEO

555 Warren Road, Ithaca, NY 14850
607-257-1551, ext. 1001
jmatteson@tstboces.org

June 20, 2022

Tompkins-Seneca Tioga BOCES is in receipt of the Draft Network Access and Information Technology Assets Report of Examination 2022M-65. Prior to receipt of the draft, the BOCES began implementing recommendations based on informal conversations with the audit team.

BOCES officials generally agreed with the recommendations in the draft and have initiated the following:

- In process - writing a technology procedures guide with a section on managing network user accounts
- Completed – unneeded user accounts have been disabled and a tool has been put in place to monitor account activity and review them for viability and removal on a weekly basis
- Completed – historical data is now preserved for our IT Security Awareness training and monitoring and tailoring of the training has been initiated and tied to the individual employee's risk factors
- In process – IT asset inventory monitoring and record management procedures are under development

The BOCES wishes to thank the audit team for their diligence in identification of potential improvements to our voluntary IT training program and our user accounts and inventory. Although there were no improprieties identified, the findings and recommendations are useful to the organization in ensuring that our IT assets are managed efficiently and our IT security is sound.

Thank You,

Dr. Jeffrey A. Matteson
District Superintendent
Tompkins-Seneca-Tioga BOCES

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 interviewed BOCES officials and reviewed the Board meeting minutes, resolutions, policies, and additional guidelines to gain an understanding of the network access and IT asset policies, procedures and guidelines.
- We ran a computerized audit script on December 8, 2021, reviewed all 436 enabled network user accounts identified by the script and compared them to the current employee list to identify inactive and other possibly unneeded accounts. We then discussed all identified non-employee accounts with the Coordinator to determine if the accounts were needed or should have been disabled.
- We discussed and reviewed the security awareness and cybersecurity training processes in place at BOCES with the Coordinator and officials. We reviewed available security awareness testing data from October 2021 through December 2021 to quantify which employees did not pass and how often.
- We obtained the BOCES' IT asset inventory records and compared them to physical IT assets present at the main campus. For assets that we were unable to locate, we reviewed disposal records and requested assistance from BOCES officials to help locate the assets.
- We tracked physical IT assets located at the BOCES main campus to the inventory list to determine whether they were accurately recorded.

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 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 by posting it to the BOCES' website.

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

BINGHAMTON REGIONAL OFFICE – Ann C. Singer, Chief Examiner

State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417

Tel (607) 721-8306 • Fax (607) 721-8313 • Email: Muni-Binghamton@osc.ny.gov

Serving: Broome, Chemung, Chenango, Cortland, Delaware, Otsego, Schoharie, Tioga, Tompkins counties

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