DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2020M-99

Oneida-Herkimer-Madison Board of Cooperative Educational Services

Information Technology

DECEMBER 2020

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

Contents

Report Highlights

Oneida-Herkimer-Madison Board of Cooperative Educational Services

Audit Objective

Determine whether Oneida-Herkimer-Madison Board of Cooperative Educational Services (BOCES) officials ensured:

- Security awareness training was provided,
- Information technology (IT) assets were accessed for appropriate purposes, and
- IT controls over BOCES' network and financial system were adequate to safeguard information.

Key Findings

BOCES officials did not regularly provide formalized IT security awareness training, assess computer usage to confirm IT assets were used for appropriate purposes or establish adequate controls to safeguard information contained in the network and financial system.

- Personal Internet use was found on computers.
- Network and application user accounts were not properly managed.
- No Disaster Recovery Plan was developed.

Sensitive IT control weaknesses were communicated confidentially to BOCES officials.

Key Recommendations

- Provide periodic IT security awareness training.
- Monitor employee Internet use.
- Develop stronger IT controls.

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

Background

BOCES is composed of 12 component school districts. BOCES is governed by a 12-member Board of Education (Board), with a member elected by each 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 Director of Information and Technology (Director) is responsible for managing BOCES' IT operations and reports to the Superintendent.

Quick Facts	
Employees	738
Student Enrollment	1,325
Total Network Accounts	2,586
Nonstudent Network Accounts	1,013

Audit Period

July 1, 2018 – February 12, 2020

Information Technology

BOCES relies on its IT assets for Internet access, email and maintaining financial information which contains personal, private and sensitive information (PPSI).[1] BOCES contracts with the Mohawk Regional Information Center (MORIC) for Internet access and filtering, data privacy and security, firewall services, data support services, access to library services and student information system support. The Director, along with six full-time IT employees, are responsible for overseeing general computer system operations.

Why Should BOCES Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, BOCES officials should provide periodic IT security awareness training. This training should explain the proper rules of behavior for using the Internet, IT systems, data and PPSI. The training also should communicate related policies and procedures to all employees using IT resources and explain the consequences of policy violations. The training should center on emerging trends such as information theft, social engineering attacks[2] and computer viruses, and other types of malicious software, all of which may result in PPSI compromise or expose BOCES to ransomware attacks.

Training programs should be directed at the specific audience (e.g., system users or administrators) and include everything that attendees need to perform their jobs. Training programs should also cover key security concepts, such as the dangers of Internet browsing and downloading files and programs from the Internet, requirements related to protecting PPSI, the importance of selecting strong passwords, and how to respond if a cyber incident is detected.

BOCES Did Not Provide Periodic IT Security Awareness Training to All IT Users

Prior to our audit fieldwork, BOCES did not provide employees with any formalized IT security awareness training to ensure they understood security measures needed to protect the network, despite its own written policy that requires staff be provided with this training.

This lack of training may have contributed to a ransomware attack that BOCES sustained in July 2019. While BOCES was able to restore its network without paying a ransom, BOCES did experience an interruption of service for a short period of time. BOCES also did not immediately implement a security awareness

Lack of training may have contributed to a ransomware attack that BOCES sustained in July 2019.

[1] PPSI is any information to which unauthorized access, disclosure, modification, destruction or use – or disruption of access or use—could have or cause a severe impact on critical functions, employees, customers (component school districts and students), third parties or other individuals or entities.

[2] Social engineering attacks are methods used to deceive users into revealing confidential or sensitive information.

training program, though it provided a computer-based IT security awareness training to employees beginning in December 2019. Officials told us that they planned to launch additional trainings in the near future; however, they did not establish specific plans to provide periodic, formal security trainings to all employees.

The IT cybersecurity community identifies people as the weakest link in the chain to secure data and IT systems. BOCES officials cannot protect the confidentiality, integrity and availability of data and computer systems without ensuring that employees understand their roles and responsibilities related to IT and data security. Without periodic, formal security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise IT assets. As a result, data and PPSI could be at greater risk for unauthorized access, misuse or abuse.

How Does an Acceptable Use Policy (AUP) Protect IT Assets?

A BOCES should have a written AUP that defines the procedures for computer, Internet and email use. The AUP should describe what constitutes appropriate and inappropriate use of IT resources, management's expectations concerning personal use of IT equipment and user privacy and consequences for violating the AUP. Monitoring compliance with the AUP involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity.

Internet browsing increases the likelihood that users will be exposed to malicious software, known as malware[3] that may compromise data confidentiality, integrity or availability. BOCES officials can reduce the risks to IT assets by routinely monitoring Internet usage and by configuring web-filtering software to block access to unacceptable websites and help limit access only to websites that comply with the AUP.

BOCES' AUP indicates that staff may only use the IT assets for the purpose of performing their work duties, and that access rights are limited to the scope of each user's job responsibility. The AUP further provides that while limited personal use for brief communication with family members may be acceptable, use of the IT assets for any other purpose may be classified as unacceptable work performance. The AUP specifies the following activities as inappropriate: conducting business transactions not related to their school responsibilities; downloading or installing any program, application, content or other software that has not been approved for installation by BOCES; and participating in email communication that is not specifically permitted as a legitimate school-related purpose.

[3] Common examples of malware include viruses, worms, Trojan horses and spyware.

Some BOCES Computers Were Used for Personal Activities

We reviewed the Internet browsing history on two servers and 21[4] user computers assigned to 16 employees whose job duties required them to have administrative access rights to BOCES' network and user computers, or had access to PPSI or other confidential information. We identified 15 employees who accessed websites not related to BOCES business.[5] Eight of these employees − from various departments, including IT, the Central Business Office, Human Resources and Administrative Services − had accessed websites not related to BOCES business and used BOCES computers for significant personal use.

We identified 15 employees who accessed websites not related to BOCES business.

Employees' personal use included accessing websites related to personal shopping, casinos, alcohol, online banking, bill paying, web searches for non-BOCES related subjects, entertainment, personal email and social media. For example, one IT employee, with administrative permissions to make system-wide changes, showed significant amounts of the aforementioned personal Internet uses and also accessed websites related to e-cigarettes, guns and sports betting. This employee also attempted to download and install unapproved software/applications not associated with BOCES operations.

BOCES officials told us that a web filter was in place to monitor Internet activities. While a web filter allows for restricting and blocking access to known prohibited websites, the web filter should also maintain a log of websites visited by users which should be periodically reviewed for appropriateness and compliance with the AUP to ensure users are not accessing websites restricted in the AUP. IT officials relied solely on the web filtering and did not routinely monitor usage logs to identify the inappropriate Internet use as outlined in BOCES' policy.

The AUP indicated that inappropriate personal use may be "classified as unacceptable work performance, and may be subject to counseling or discipline consistent with applicable laws and collective bargaining agreements," and employees are required to sign an acknowledgment of the AUP. However, the Director acknowledged that officials have done little to monitor and enforce compliance with the AUP.

Internet browsing increases the likelihood of computers being exposed to malicious software that may compromise PPSI. As a result, BOCES' IT assets and any PPSI they contain have a higher risk of exposure to damage and PPSI breach, loss or misuse. Additionally, when employees use BOCES resources to access websites for non-BOCES business activities, productivity may be reduced.

[4] Of the 21 user computers, we were unable to obtain web history data from one computer because the device's hardware specification was insufficient for our audit script to be run.

[5] We were unable to determine the browsing history for one user because the website history had been deleted.

Why Should BOCES Properly Manage User Accounts and Permissions?

User accounts provide access to network resources and financial applications and should be actively managed to minimize the risk of misuse. If not properly managed, user accounts could be potential entry points for attackers because they could be used to inappropriately access and view PPSI on the network and in the financial system. A BOCES should have written procedures for granting, changing and revoking access rights to the network and to the financial application.

In addition, to minimize the risk of unauthorized access, BOCES officials should regularly review enabled network and financial application user accounts to ensure that users are still employed by BOCES and access rights are still appropriate to their current job. Officials must disable unnecessary accounts/rights as soon as there is no longer a need for them.

Because shared accounts are not assigned to a single user, officials may have difficulty managing these accounts and linking any suspicious activity to a specific user. To help ensure individual accountability, all users should have and use their own user account to gain access to a network and applications. If shared accounts are necessary, officials should have procedures in place to monitor who uses the accounts and when they are used.

IT managers should establish user accounts with specific user permissions needed by each individual to perform their job functions. This ensures access to PPSI is restricted to only those individuals who are authorized to access it.

BOCES' policy states that BOCES will periodically review the roster of users and their assigned access rights, and make adjustments to reflect any changes in circumstances. The policy further authorizes the Superintendent, in consultation with the IT Director, to develop and adopt procedures and protocols for assigning, reviewing and removing user access rights.

Officials Did Not Adequately Manage User Accounts and Permissions.

We reviewed 1,013 enabled non-student user accounts on BOCES' network, and all 70 financial application user accounts. BOCES officials did not adequately manage user accounts and permissions for BOCES' network and the financial application as follows:

<u>Former Employees and Consultants</u> − During our review of network accounts, we found 134 enabled, active network accounts that were assigned to former employees or consultants. Of these, 72 had never been used to log onto the network and 26 were last accessed between November 1, 2012 and April 30, 2018. User accounts of former employees and consultants that have not been

disabled or removed could potentially be used by those individuals or others for malicious purposes.

Shared Accounts − During our review of network accounts, we found 93 shared network user accounts that had varied purposes, ranging from administrative functions such as accounts used to set up phone services; instructional purposes such as accounts used by summer school teachers to give temporary access to computer devices and basic applications; and accounts used to access servers and configure web filtering settings.

Of the 93, BOCES officials told us 75 were unnecessary and the remaining 18 were necessary. However, nine of the 18 necessary accounts were shared among multiple unspecified users. Officials did not have procedures in place to monitor who used these nine shared accounts. Therefore, it may not always be clear who uses the accounts and whether use is for a legitimate purpose. As a result, BOCES has a greater risk that PPSI could be changed intentionally or unintentionally, or used inappropriately, and officials would not be able to identify who performed the unauthorized activities.

Thirty-eight users had unnecessary user permissions that allowed them to access other employees' social security numbers, and six users had unnecessary user permissions to modify employee salaries.

Software Application User Accounts − We reviewed user permissions of all 70 user accounts for BOCES' financial application and found that 12 former employees or third-party consultants who were no longer associated with BOCES had active user access to the application. Further, 38 users had unnecessary user permissions that allowed them to access other employees' social security numbers,[6] and six users had unnecessary user permissions to modify employee salaries. These users did not need these user permissions to fulfill their job duties.

BOCES officials did not have written procedures for granting, changing and revoking access rights to BOCES' network and financial application. In addition, officials did not regularly review user accounts to ensure they had appropriate user permissions. As a result, the 134 unneeded network accounts, 75 shared accounts, 12 financial application accounts and unnecessary user permissions went unnoticed until our audit.

Because BOCES' network had unneeded enabled user accounts, it had a greater risk that these accounts could have been used as entry points for attackers to access PPSI and compromise IT resources. In addition, because BOCES users of the financial application had unnecessary user permissions, BOCES had an increased risk that employees' PPSI could be used to commit fraud and/or identity theft and that it would be liable for losses incurred.

[6] We notified BOCES officials and they removed access.

Why Is It Important To Maintain an Inventory and Identify Users of PPSI?

Data classification is the process of identifying and categorizing data to help officials make informed decisions about how to properly protect it. Data classification includes scanning data repositories and organizing the data to determine what it is, where it is located and how to protect it.

BOCES officials should classify BOCES data to properly identify where PPSI is stored and how to adequately protect it. Classifying the PPSI data and users can help identify the type of security controls appropriate for safeguarding and disseminating the data. In addition, PPSI policies should include consequences or escalation procedures for noncompliance.

BOCES has a written policy that identifies information that it considers PPSI, which includes personally-identifiable information, and addresses procedures to follow should there be a data breach or PPSI compromise. This policy is posted on BOCES' website. However, BOCES does not have any written policy that addresses protecting, inventorying and classifying PPSI or defining a level of security to be applied to each classification of PPSI data.

PPSI Was Not Properly Managed

BOCES uses its computer system to collect and store data received and produced from its operations, which includes PPSI and other confidential financial, student and employee data. Although a BOCES policy indicated what type of information that BOCES considered PPSI, we found that BOCES did not classify or maintain an inventory of BOCES' PPSI data itself and where PPSI is stored in the computer system. Further, BOCES' policies did not identify the specific users of PPSI.

The Director told us that BOCES has implemented a system for delivery of documents or data that contain PPSI and that students' records are not transferred through online methods. However, the Director acknowledged that BOCES had no PPSI inventories or written policies that classify PPSI or provide different levels of security to be applied to each classification of PPSI data. Without a PPSI inventory, BOCES cannot ensure that all PPSI is properly accounted for and protected from improper data changes or deletions, unauthorized system access and data breaches.

BOCES had no PPSI inventories or written policies that classify PPSI or provide different levels of security to be applied to each classification of PPSI data.

Why Should BOCES Have a Disaster Recovery Plan?

To minimize the risk of data loss or suffering a serious interruption of services, BOCES officials should establish a formal written disaster recovery plan (plan). The plan should address the potential for sudden, unplanned catastrophic events, (e.g., fire, computer virus or inadvertent employee action) that could compromise the network and the availability or integrity of BOCES' IT system and data, including its financial application and any PPSI contained therein. Typically, a plan involves analyzing business processes and continuity needs, identifying roles of key individuals and necessary precautions to take to maintain or quickly resume operations.

A backup is a copy of data files and software programs made to replace original versions if there is loss or damage to the original. A plan should include data backup procedures, such as ensuring a backup is stored at a secure offsite location, encrypted and periodically tested to ensure its integrity and that it will function as expected.

The plan should be tested periodically and updated to ensure officials understand their roles and responsibilities in a disaster situation and to address changes in security requirements.

BOCES Did Not Have a Disaster Recovery Plan

The Board did not develop and implement a plan to address potential disasters. Consequently, in the event of a disaster, officials do not have guidelines to minimize or prevent the loss of equipment and data or to appropriately recover data.

BOCES officials told us that they back up data regularly, and backups are periodically moved to an offsite storage. BOCES rarely does a full backup of all BOCES' data; rather, data is backed up individually as needed. Because BOCES does not have a plan, personnel have no guidance to minimize the loss of IT equipment and data or implement data recovery in the event of a disaster. While the Director told us that BOCES was in the process of drafting a plan, it had not been finalized as of the end of fieldwork.

Without a comprehensive plan, BOCES could lose important financial and other data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees or process State aid claims.

What Do We Recommend?

BOCES officials should:

1. Provide employees with periodic IT security awareness training.

2. Develop written procedures for granting, changing and revoking access rights to the network and financial application.

3. Assess user permissions for all financial application users and remove excessive user permissions for those users who do not need that level of access to perform their job duties.

The Director should:

4. Monitor employee Internet use to ensure compliance with the AUP.

5. Evaluate all existing network accounts and immediately disable any network user accounts that are not needed. Going forward, disable network accounts of former employees and consultants as soon as they leave BOCES employment, and routinely review network user accounts and disable those that are no longer needed.

6. Restrict the use of shared network user accounts and develop procedures to monitor who uses these accounts.

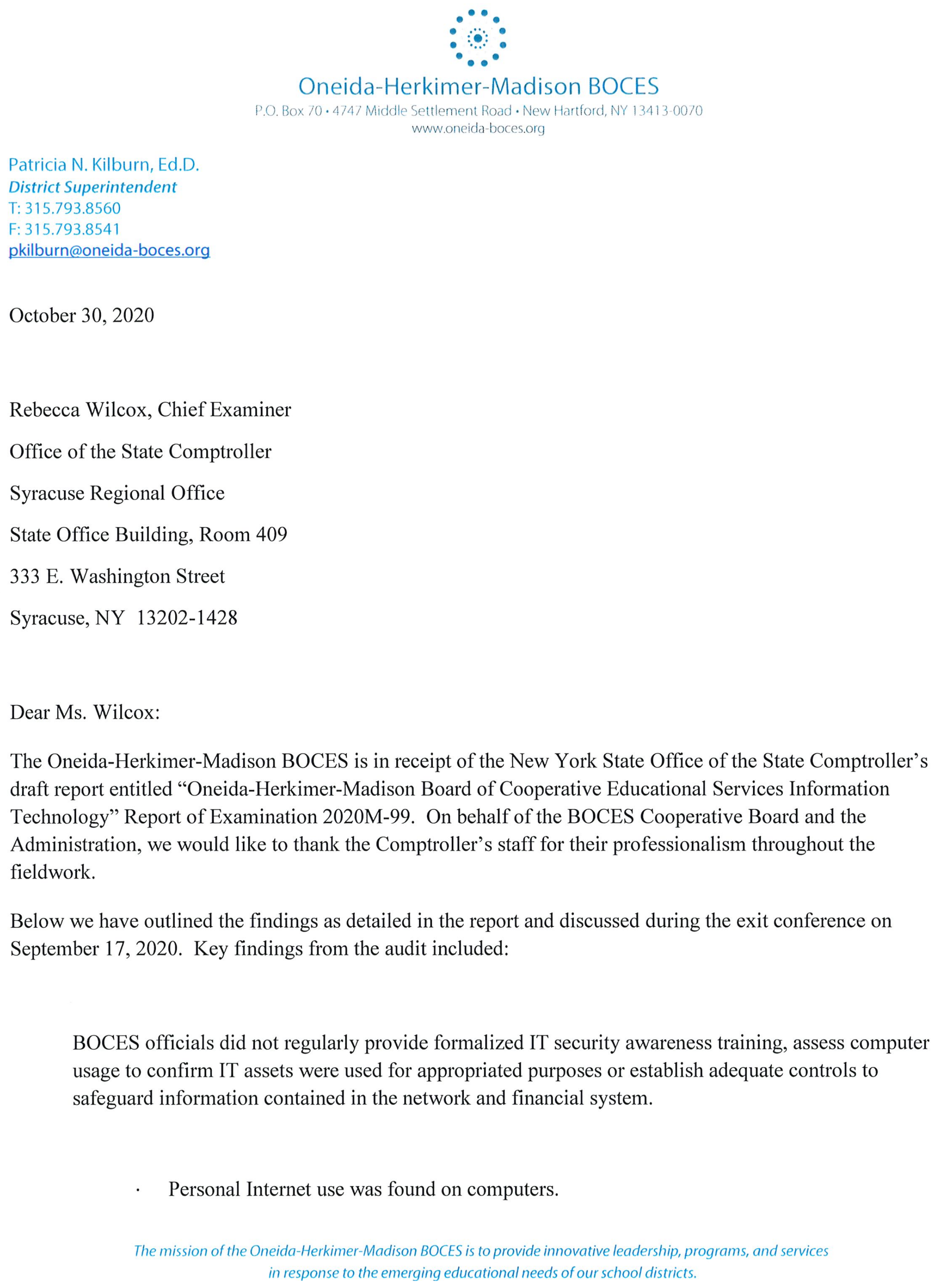
7. Develop a PPSI inventory by classifying all BOCES data and identifying where it is stored in the computer system and who uses it. Also, periodically review and update the inventory.

The Board should:

8. Ensure BOCES officials monitor and enforce employee compliance with BOCES policies, including policies related to the use of and access to the computer system, PPSI and other sensitive data.

9. Develop a comprehensive written disaster recovery plan and ensure it is distributed to all responsible parties, periodically tested and updated as needed.

Appendix A: Response From BOCES Officials



Oneida-Herkimer-Madison BOCES
P.O. Box 70 • 4747 Middle Settlement Road • New Hartford, NY 13413-0070
www.oneida-boces.org

Patricia N. Kilburn, Ed.D.
District Superintendent
T: 315.793.8560
F: 315.793.8541
pkilburn@oneida-boces.org

October 30, 2020

Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
Syracuse Regional Office
State Office Building, Room 409
333 E. Washington Street
Syracuse, NY 13202-1428

Dear Ms. Wilcox:

The Oneida-Herkimer-Madison BOCES is in receipt of the New York State Office of the State Comptroller's draft report entitled "Oneida-Herkimer-Madison Board of Cooperative Educational Services Information Technology" Report of Examination 2020M-99. On behalf of the BOCES Cooperative Board and the Administration, we would like to thank the Comptroller's staff for their professionalism throughout the fieldwork.

Below we have outlined the findings as detailed in the report and discussed during the exit conference on September 17, 2020. Key findings from the audit included:

> BOCES officials did not regularly provide formalized IT security awareness training, assess computer usage to confirm IT assets were used for appropriated purposes or establish adequate controls to safeguard information contained in the network and financial system.

- Personal Internet use was found on computers.

- Network and application user accounts were not properly managed.
- No Disaster Recovery Plan was developed.

Administration and the Cooperative Board do not dispute the findings and we are appreciative of the examination of our systems and the feedback that will be used to address areas in need of improvement. A number of the items have been addressed since the audit including; IT security awareness training, better management of network and application access, and the development of a formal Disaster Recovery Plan which was approved by the Board at its May 2020 meeting.

With regard to the findings related to the use of BOCES hardware and networks for appropriate purposes and personal internet use we acknowledge these findings as accurate. However, we do note that Policy #5306 includes the following language; "Limited personal use for such purposes as brief communication with family may be acceptable, but staff members should keep in mind that any data created by personal use remains subject to review by the OHM BOCES."

The BOCES is thankful for the opportunity to receive valuable feedback to improve our policies and practices related to information security and privacy measures.

Sincerely,

Patricia N. Kilburn, Ed.D.

District Superintendent

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 employees and reviewed BOCES' IT policies to gain an understanding of BOCES' IT environment and internal controls and to determine whether BOCES has developed a written disaster recovery plan.
- We interviewed BOCES officials to determine whether employees received periodic and organized IT security awareness training. We also reviewed IT security awareness training progress reports to identify whether required staff received and completed the training.
- We reviewed user account permissions for all 70 users of BOCES' financial application and determined whether they were appropriate based on job functions and required access to sensitive data.
- We reviewed Internet browsing history on two servers and 21 user computers assigned to 16 employees to evaluate whether their Internet browsing use was in compliance with the AUP. Of the 21 user computers, we were unable to obtain Internet browsing history data from one computer because the device's hardware specification was insufficient for our audit script to be run. We also reviewed the local security settings on these servers and user computers. We used our professional judgment to select the 16 employees because they had either administrative access to the network and IT system or access to financial and employee records.
- We provided the Director with a computerized audit script to run and analyzed the reports produced to assess network user accounts and security settings applied to those accounts.
- We compared BOCES' employee master and payroll list reports to names of account users listed in the audit script report to determine whether all users with enabled network accounts were currently employed or contracted by BOCES.

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 GAGAS (generally accepted government auditing standards). 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 to BOCES' 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

SYRACUSE REGIONAL OFFICE – Rebecca Wilcox, Chief Examiner

State Office Building, Room 409 • 333 E. Washington Street • Syracuse, New York 13202-1428

Tel (315) 428-4192 • Fax (315) 426-2119 • Email: Muni-Syracuse@osc.ny.gov

Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence counties

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