DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2020M-95

Susquehanna Valley Central School District

Information Technology

OCTOBER 2020

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

Contents

Report Highlights

Susquehanna Valley Central School District

Audit Objective

Determine whether Susquehanna Valley Central School District (District) officials established information technology (IT) controls over user access to protect against unauthorized use, access and loss.

Key Findings

District officials did not establish adequate IT controls over user access to protect against unauthorized use, access and loss. District officials did not:

- Adequately manage user accounts including periodically reviewing and disabling unneeded network user accounts.
- Maintain accurate, complete and up-to-date hardware and software inventory.
- Ensure that computers were free from malicious software. In fact, two malicious software applications were installed on District computers.

Sensitive IT control weaknesses were communicated confidentially to officials.

Key Recommendations

- Develop comprehensive procedures for regularly reviewing user accounts and disabling those that are unnecessary.
- Maintain an accurate, complete and up-to-date hardware and software inventory.
- Adopt and monitor comprehensive IT security policies.

District officials agreed with our recommendations and have initiated or indicated they planned to initiate corrective action.

Background

The District serves the Towns of Binghamton, Conklin, Kirkwood, Vestal and Windsor in Broome County.

The District is governed by a seven-member Board of Education (Board) responsible for the general management and control of financial and educational affairs. The Superintendent of Schools is the chief executive officer responsible for District administration.

The Director of Technology/Chief Information Officer (Director) is the network administrator responsible for the overall management of IT infrastructure. The District also contracted with the Broome-Tioga Board of Cooperative Educational Services (BT BOCES) to provide IT services.

Quick Facts	
Network User Accounts	2,407
Desktop, Laptop and Tablet Computers	1,982
Employees	323
Enrollment	1,418

Audit Period

July 1, 2018 – March 9, 2020

Information Technology

Why Should District Officials Manage User Accounts?

Network user accounts enable the system to recognize specific users, grant authorized access rights and provide accountability by affiliating user accounts with specific users. However, user accounts are potential entry points for attackers because they could be inappropriately used to access data and view personal, private and sensitive information (PPSI).[1]

A district should have written procedures for granting, changing and revoking user access to its network. To minimize the risk of unauthorized access, district officials should regularly review enabled network accounts to ensure they are still needed. Officials must disable unnecessary accounts as soon as there is no longer a need for them.

To minimize the risk of unauthorized access, district officials should regularly review enabled network accounts to ensure they are still needed.

A shared user account is a network, local or application user account with a username and password that is shared among two or more people. Shared accounts are often used to provide access to guests and temporary or intermittent IT users (e.g., substitute teachers and third-party vendors) and automated processes (e.g., backups and testing).

To the extent possible, all users should have and use their own user accounts to gain access to networks, computers and applications. If district officials allow users to share accounts, officials should track each user's activity while using the shared accounts. This helps ensure accountability over work performed and data changed or deleted.

When shared accounts are not properly managed, officials may have difficulty linking any suspicious activity to a specific user and detecting and disabling unneeded accounts in a timely manner. Officials also should routinely evaluate shared user accounts and disable those that are no longer needed. This helps limit the possibility that PPSI may become compromised.

Officials Did Not Adequately Manage User Accounts

District officials did not develop written procedures for managing, limiting and monitoring user accounts and securing PPSI. The Director and BT BOCES staff managed and maintained the District's network access. The District secretary added network user access, and the Director and BT BOCES staff removed and modified user access of the network.

[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, third-parties or other individuals or entities.

We examined all 454 non-student network user accounts and found the following questionable or unneeded accounts:[2]

- 37 accounts (8 percent) assigned to current employees had not been used in at least six months. These accounts were for bus attendants and drivers, substitute teachers, support staff, coaches, a food service helper, a cook, a custodian, guidance counselor, a teacher aide and a courier. The accounts were provided to these individuals for functions such as checking emails but were not used routinely and were not needed for ongoing email access. The Director told us that 19 of these accounts were no longer necessary.
- 58 accounts (13 percent) did not match the list of current employees and appeared to be unnecessary. Of these accounts, the following 46 accounts had not been used in at least six months: 41 were assigned to former employees, two assigned to BT BOCES employees were no longer needed and three were test accounts. The Director disabled 46 of these user accounts during our audit fieldwork.
- 56 accounts (12 percent) were not assigned to specific individuals and not needed. Of these accounts, 44 had not been used in at least six months. Furthermore, 11 of the 56 accounts were associated with the set-up of computers and computer functions and had not been used for more than three years. The Director told us that these 11 accounts could be disabled, and that 27 of the 56 accounts were created solely for an email account but were not needed for ongoing email access. Therefore, we question the need for any of these accounts. The Director disabled 30 of these accounts while we were onsite.

58 accounts (13 percent) did not match the list of current employees and appeared to be unnecessary.

The Director told us that they did not have any written procedures for monitoring user accounts and were unable to trace activity of shared accounts to a specific user. Furthermore, they may be able to deactivate the active directory account and keep the email account active.[3]

Officials should disable any unneeded network accounts as soon as they are no longer needed. These actions decrease the risk of unauthorized access and potential entry points for attackers to compromise IT resources. Furthermore, when the District allows users to use shared accounts, the ability to hold

[2] We did not review the network user account settings for 1,953 student accounts. The accounts we reviewed included all current and former District employees, current and former BT BOCES employees and generic accounts. Generic accounts are used for certain network services to run properly and can be created for services that are not linked to a personal account to meet various business needs. For example, generic accounts can be used for training purposes or as a generic email account, such as a service helpdesk account. Generic accounts that are not related to specific system needs should be routinely evaluated and disabled, if deemed unnecessary. Refer to Appendix B for information on our methodology.

[3] Active directory is a directory service that provides management for all users, computers, software and security within a network or computer system.

individuals accountable is diminished. If problems occurred, officials could have difficulty holding users accountable and taking disciplinary action because any user could blame their activity on another user.

Why Should Officials Maintain Accurate Hardware and Software Inventories?

Computer hardware and software management is essential to safeguarding district assets and data. District officials should maintain detailed, up-to-date inventory records for all computer hardware to safeguard IT assets. Reliable IT inventory records are critical for protecting these assets from theft, loss or misuse. District officials cannot properly track and protect IT assets if they do not know what IT assets they have and where those assets reside. The failure to maintain detailed, up-to-date hardware and software inventories exposes these valuable assets to an increased risk of loss, theft or misuse, putting district data at risk.

Information maintained for each piece of computer equipment should include a description of the item, name of the employee to whom the equipment is assigned, physical location of the equipment and relevant purchase or lease information. Officials should verify the accuracy of inventory records through periodic physical inventory counts.

Software inventory records should include software application descriptions, versions and serial numbers; description and location of computers on which the software is installed; and pertinent licensing information. Effective software management also includes ensuring that only appropriate business software is installed to reduce the risk of unwanted consequences and unnecessary costs that could result from unauthorized software. Maintaining complete and up-to-date hardware and software inventories helps the board develop formal IT replacement plans.

Officials Did Not Maintain Accurate and Complete Hardware or Software Inventories

The Director maintained a hardware inventory that included devices, models, serial numbers and inventory tags. The Director also maintained a software inventory that included the software name and a brief description of its purpose. However, we found the District's hardware and software inventory records were not accurate, complete or up-to-date.

Hardware Inventory – We reviewed the hardware inventory and found that eight computers had no inventory tag associated with them. We compared the District's hardware inventory list to the inventory list provided by BT BOCES and found that five computers were not on the District's list.

...[T]he District's hardware and software inventory records were not accurate, complete or up-to-date.

When we attempted to compare 19 computers located at the District to the District's hardware inventory list, we were unable to identify three computers (a desktop, a tablet and a laptop) because they did not have inventory tags affixed to them. In addition, we surveyed all District employees for computer equipment issued to them by the District and received 170 employee responses, which identified 352 computers issued.

However, we were unable to determine whether 114 of these computers were on the District's inventory because the list was incomplete. For example, the list did not always specify to whom the computer equipment was assigned. Because District officials did not maintain up-to-date hardware inventory records, there is an increased risk that IT assets may be lost, stolen or misused.

Software Inventory – We reviewed the software installed on 15 computers (eight desktops and seven laptops) and found that 19 software applications were not on the software inventory list. Two installed applications – one on the Director's laptop and one on the Superintendent's laptop – were malicious software (malware).[4]

Two installed applications – one on the Director's laptop and one on the Superintendent's laptop – were malicious software...

Without a complete and comprehensive software inventory, officials have no assurance that all installed software is for proper purposes and there is an increased risk that installed malware may not be detected timely. Malware can corrupt data and make devices inoperable, be expensive to fix and can cause significant losses in productivity until corrected.

The Board adopted policies related to IT, including computer usage and internet security, confidentiality of computerized information and information security breach and notification. However, these deficiencies occurred, in part, because the policies did not adequately address user access management or hardware and software inventories.

Although the District's computer usage and internet security policy addressed rules for users, it did not address managing all user accounts and hardware assigned to staff. In addition, because officials did not maintain detailed, up-to-date hardware and software inventory records, the District had an increased risk that its IT assets may be lost, stolen or misused.

[4] Malware is malicious software and common examples include viruses, worms, Trojan horses and spyware.

What Do We Recommend?

The Director should:

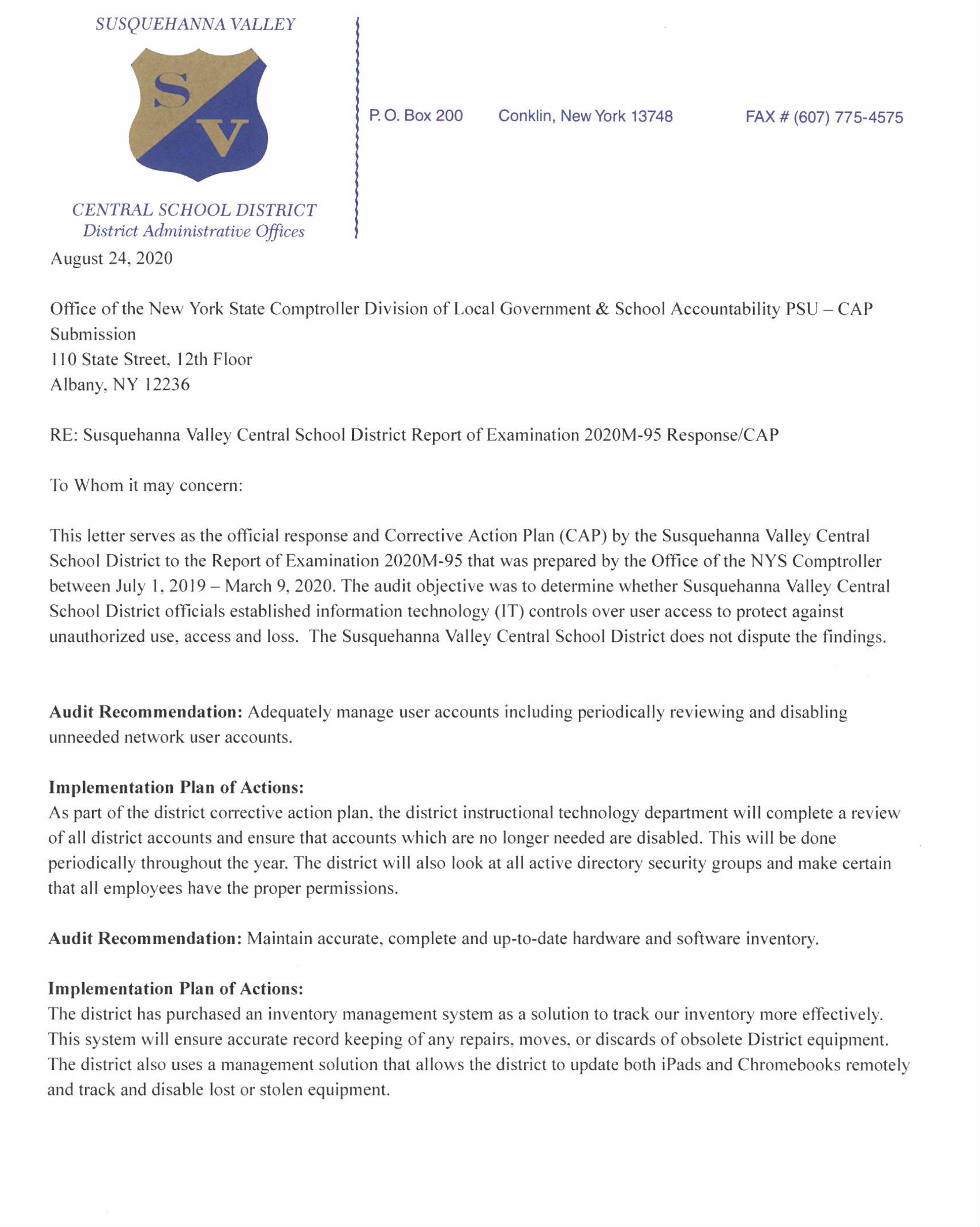
1. Routinely evaluate user accounts and disable those that are no longer needed.

2. Develop comprehensive up-to-date hardware and software inventory lists that include locations of the equipment, names of individual assigned the equipment and the software installed on each device.

The Board should:

3. Adopt and periodically review and update comprehensive IT security policies for user accounts and hardware and software inventory.

Appendix A: Response From District Officials



SUSQUEHANNA VALLEY

S V

CENTRAL SCHOOL DISTRICT
District Administrative Offices

P. O. Box 200 Conklin, New York 13748 FAX # (607) 775-4575

August 24, 2020

Office of the New York State Comptroller Division of Local Government & School Accountability PSU – CAP Submission
110 State Street, 12th Floor
Albany, NY 12236

RE: Susquehanna Valley Central School District Report of Examination 2020M-95 Response/CAP

To Whom it may concern:

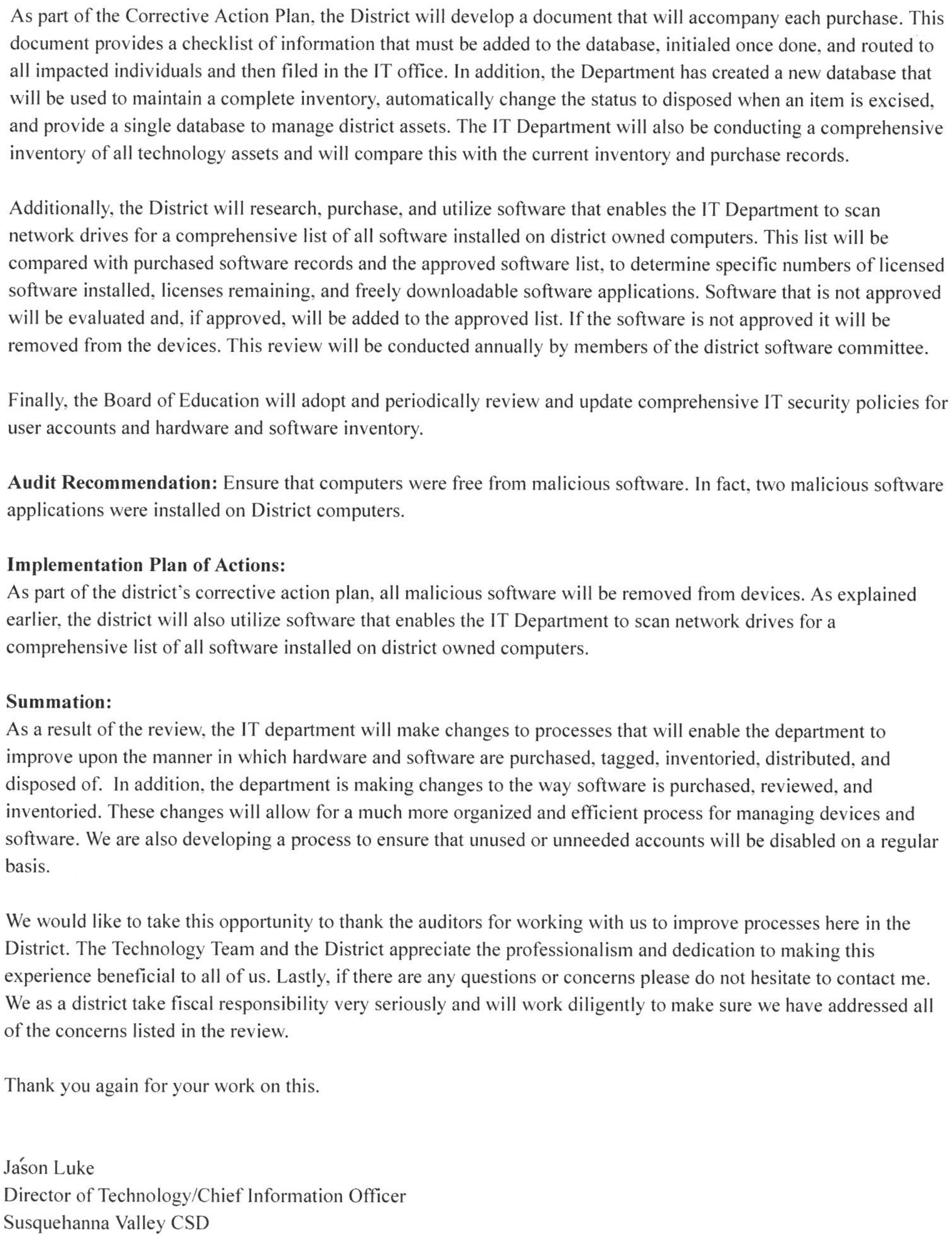
This letter serves as the official response and Corrective Action Plan (CAP) by the Susquehanna Valley Central School District to the Report of Examination 2020M-95 that was prepared by the Office of the NYS Comptroller between July 1, 2019 – March 9, 2020. The audit objective was to determine whether Susquehanna Valley Central School District officials established information technology (IT) controls over user access to protect against unauthorized use, access and loss. The Susquehanna Valley Central School District does not dispute the findings.

Audit Recommendation: Adequately manage user accounts including periodically reviewing and disabling unneeded network user accounts.

Implementation Plan of Actions:
As part of the district corrective action plan, the district instructional technology department will complete a review of all district accounts and ensure that accounts which are no longer needed are disabled. This will be done periodically throughout the year. The district will also look at all active directory security groups and make certain that all employees have the proper permissions.

Audit Recommendation: Maintain accurate, complete and up-to-date hardware and software inventory.

Implementation Plan of Actions:
The district has purchased an inventory management system as a solution to track our inventory more effectively. This system will ensure accurate record keeping of any repairs, moves, or discards of obsolete District equipment. The district also uses a management solution that allows the district to update both iPads and Chromebooks remotely and track and disable lost or stolen equipment.



As part of the Corrective Action Plan, the District will develop a document that will accompany each purchase. This document provides a checklist of information that must be added to the database, initialed once done, and routed to all impacted individuals and then filed in the IT office. In addition, the Department has created a new database that will be used to maintain a complete inventory, automatically change the status to disposed when an item is excised, and provide a single database to manage district assets. The IT Department will also be conducting a comprehensive inventory of all technology assets and will compare this with the current inventory and purchase records.

Additionally, the District will research, purchase, and utilize software that enables the IT Department to scan network drives for a comprehensive list of all software installed on district owned computers. This list will be compared with purchased software records and the approved software list, to determine specific numbers of licensed software installed, licenses remaining, and freely downloadable software applications. Software that is not approved will be evaluated and, if approved, will be added to the approved list. If the software is not approved it will be removed from the devices. This review will be conducted annually by members of the district software committee.

Finally, the Board of Education will adopt and periodically review and update comprehensive IT security policies for user accounts and hardware and software inventory.

Audit Recommendation: Ensure that computers were free from malicious software. In fact, two malicious software applications were installed on District computers.

Implementation Plan of Actions:
As part of the district's corrective action plan, all malicious software will be removed from devices. As explained earlier, the district will also utilize software that enables the IT Department to scan network drives for a comprehensive list of all software installed on district owned computers.

Summation:
As a result of the review, the IT department will make changes to processes that will enable the department to improve upon the manner in which hardware and software are purchased, tagged, inventoried, distributed, and disposed of. In addition, the department is making changes to the way software is purchased, reviewed, and inventoried. These changes will allow for a much more organized and efficient process for managing devices and software. We are also developing a process to ensure that unused or unneeded accounts will be disabled on a regular basis.

We would like to take this opportunity to thank the auditors for working with us to improve processes here in the District. The Technology Team and the District appreciate the professionalism and dedication to making this experience beneficial to all of us. Lastly, if there are any questions or concerns please do not hesitate to contact me. We as a district take fiscal responsibility very seriously and will work diligently to make sure we have addressed all of the concerns listed in the review.

Thank you again for your work on this.

Jason Luke
Director of Technology/Chief Information Officer
Susquehanna Valley CSD

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 examined the District's network user accounts and related settings using specialized audit software. We reviewed all 454 non-student network accounts and compared them to current employee lists to identify inactive and unneeded accounts. These accounts included all current and former District employees, current and former BT BOCES employees and generic accounts. We reviewed automated network settings to identify any settings that indicated ineffective IT controls.
- We reviewed the District's IT policies and procedures and interviewed District officials to gain an understanding of the District's IT operations and determine the adequacy of the policies and procedures.
- We used our professional judgment to select 11 user accounts assigned to nine employees, one student and one elementary school classroom tablet. We selected five of the 10 for our sample based on job titles that indicated duties likely to involve accessing student, staff and financial PPSI. The 11 user accounts resided on nine desktops, seven laptops and five tablets. We reviewed the Internet browsing history for all selected accounts. We used specialized audit software to obtain the Internet browsing history for the nine user accounts on the 16 computers tested (nine desktops and seven laptops). We manually observed the Internet browsing history for the five user accounts on the five tablets.
- We reviewed the District's hardware and software inventory. For our previously selected sample, we traced devices to the hardware inventory list, and (using the specialized audit software) traced software installed on those devices to the software inventory list. We surveyed all District employees to identify devices issued to them and attempted to trace those reported to us to the hardware inventory list.

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 District 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 District's 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

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, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins counties

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