New York State Comptroller
THOMAS P. DiNAPOLI

East Williston Union Free School District

Management of Nonstudent Network User Accounts

2022M-171 | June 2023

Division of Local Government and School Accountability

Contents

Report Highlights 1

Network User Accounts 2

How Should Officials Manage and Monitor Network User Accounts? . 2

Officials Did Not Adequately Manage and Monitor Network User Accounts 3

What Do We Recommend? 5

Appendix A – Response From District Officials 6

Appendix B – OSC Comment on the District's Response. 8

Appendix C – Audit Methodology and Standards 9

Appendix D – Resources and Services. 11

Report Highlights

East Williston Union Free School District

Audit Objective

Determine whether East Williston Union Free School District (District) officials adequately managed and monitored nonstudent network user accounts to help prevent unauthorized use, access and loss.

Key Findings

District officials did not adequately manage and monitor nonstudent 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:

- 222 of the enabled nonstudent network user accounts (32 percent) were not needed or disabled.

Most of these accounts should have been disabled in February 2021 when the District updated their network access requirements. However, District officials did not develop a system to communicate when a network account was no longer necessary and should be deactivated.

Key Recommendation

- Periodically review user access for all network user accounts and disable user accounts when access is no longer needed.

District officials generally agreed with our recommendations and have initiated or indicated they planned to initiate corrective action. Appendix B includes our comment on an issue that was raised in the District's response letter.

Background

The District, located in the Town of Hempstead in Nassau County, is governed by a five-member Board of Education (Board) responsible for the general management and control of financial and educational affairs.

The Director of Technology (IT Director) was appointed by the Board and is responsible for overseeing all IT functions, including network security and user accounts.

The District contracts with the Nassau Board Of Cooperative Educational Services (BOCES) for IT services (hardware, software and services required to operate and manage the technology environment), paying them $138,348 in 2020-21 fiscal year.

BOCES technicians work with the IT Director to provide network infrastructure support. One BOCES technician works onsite at the District, reporting to the IT Director and is responsible for, among other things, creating and disabling network user accounts.

Quick Facts

Enabled Network User Accounts	
Student	1,768
Nonstudent	693
Total	2,461
Employees	469
Students	1,644

Audit Period

July 1, 2020 – January 11, 2022

Network User Accounts

The District's network and data are valuable resources that are accessed by network user accounts. The District relies on its network user account access for a variety of tasks, including Internet access, email and for maintaining financial, personnel and student records, which contain personal, private, and sensitive information (PPSI).[1] If the network user account access is compromised, the results can be catastrophic and require extensive effort and resources to evaluate, repair and/or rebuild.

How Should Officials Manage and Monitor Network User Accounts?

Because user accounts provide access to the network, officials should actively manage them to minimize the risk of unauthorized use, access and loss. If not properly managed, unneeded user accounts may not be detected and disabled in a timely manner. Unneeded accounts are additional entry points for attackers to attempt to gain unauthorized access and then potentially use to inappropriately access and view PPSI, make changes to official school district records or deny legitimate access to electronic information when needed.

School district officials should establish written procedures for actively managing user accounts, including their creation, use and dormancy. User accounts should be disabled as soon as they are no longer needed, and regularly monitored to ensure they are appropriate and authorized. To accomplish this, an appropriate official should immediately notify the administrators when an account user's employment or contract is terminated so that the administrator can disable the user's accounts in all computer-related applications. Another way to accomplish this is to establish and implement a system in which network user accounts are disabled, either automatically or manually, after a reasonable specified period without a valid user account login.

To minimize the risk of unauthorized access, the IT Director should monitor network user accounts by maintaining a list of authorized user accounts and regularly reviewing enabled network user accounts to ensure they are needed.

Shared and service network user accounts should be limited in use as they are not linked to one individual and may have reduced accountability. Service accounts are accounts created for the sole purpose of running a particular network or system service or application (e.g., automated backup systems). Shared user accounts are accounts with a username and password that are shared among two or more users. Shared accounts are often used to provide access to guests and other temporary or intermittent users (e.g., substitute

[1] PPSI is any information to which unauthorized access, disclosure, modification, destruction or disruption of access or use could severely impact critical functions, students, employees, third parties or other individuals or entities.

teachers and third-party vendors). School district officials should limit the use of shared and service accounts, routinely evaluate the need for the accounts and disable those that are not related to a current district or system need.

Officials Did Not Adequately Manage and Monitor Network User Accounts

District officials did not adequately manage and monitor network user accounts. They did not establish procedures for granting, verifying, changing and disabling network user account access to ensure there were adequate controls over network user accounts for the District's network.

District officials and staff follow unwritten procedures to add and disable employee user accounts based on Board actions such as appointments and terminations of employees. When a new employee is approved by the Board, the BOCES technician creates their network user account. A staff change log is used by the IT Director and BOCES Technician to track the effective date, name and title for network accounts to be created when new employees are hired.

The IT Director said he updates and reviews the staff change log after each Board meeting and the BOCES technician said he reviews it weekly to identify new accounts to be established, or existing accounts that need to be disabled. However, network user accounts for employees who are terminated or resign should be disabled immediately. Waiting for the termination or resignation to be memorialized in the Board minutes could result in a significant amount of lag time between the separation and the disabling of the account increasing risk to the network. When a consultant network user account needs to be added or disabled, the District administrator who supervised the consultant or the Human Resources department is responsible for emailing the IT department with the applicable start and end dates. The change log is not updated to include the creation or disabling of consultant network user account changes, the email, if one is sent, is the only notification and tracking for these accounts.

Although the District had unwritten procedures in place to address new and terminated nonstudent network user accounts, we found that the IT Director did not ensure BOCES technicians followed the procedures to disable network user accounts for former employees and consultants. In addition, network user accounts were not properly monitored by the IT Director to ensure enabled network user accounts were needed.

Nearly one-third (222 of 693) of the District's nonstudent network accounts were not necessary. These nonstudent network accounts were comprised of District employees, consultants, or accounts that were shared among multiple staff, or accounts used as service connections to the District's network. While 18 of the 431 accounts (4 percent) assigned to employees or consultants were no longer needed as they had left District employment, 193 of the 217 accounts (89 percent) that were used by multiple staff were not necessary, along with 11 of 45 accounts (24 percent) that were used to service the network components. Most of the shared accounts were no longer necessary after February 2021 when the District updated their network access requirements and eliminated the need for them.

The IT Director had not developed a system to adequately communicate to BOCES personnel when a network account was no longer necessary and should be deactivated. While the 204 unnecessary shared and service accounts were disabled after we discussed them with the IT Director, the 18 unnecessary former employee and consultant network user accounts were not disabled as of the end of our fieldwork.

While effective controls do not guarantee the safety of an IT network and systems, a lack of effective controls significantly increases the risk that data, hardware, and software and the data access through the network may be lost or damaged by inappropriate access and use.

Unneeded network user accounts are additional entry points into a network and, if accessed by an attacker, could severely disrupt District operations or be used to inappropriately access the District's network to view and/or remove personal information; make unauthorized changes to District records; or deny legitimate access to the District's network and records. An attacker could use these additional entry points to severely disrupt District operations by:

- Denying District employees network access to electronic information they need to perform their job duties;
- Installing malicious software that could have a significant negative impact and/or completely shut down the District's network; and
- Obtaining and publicly releasing PPSI, such as employee and student dates of birth, home addresses and social security numbers, that could be used to facilitate identity theft.

These events could have criminal, civil, regulatory, financial and reputational impacts on District operations.

What Do We Recommend?

The Board and officials should:

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

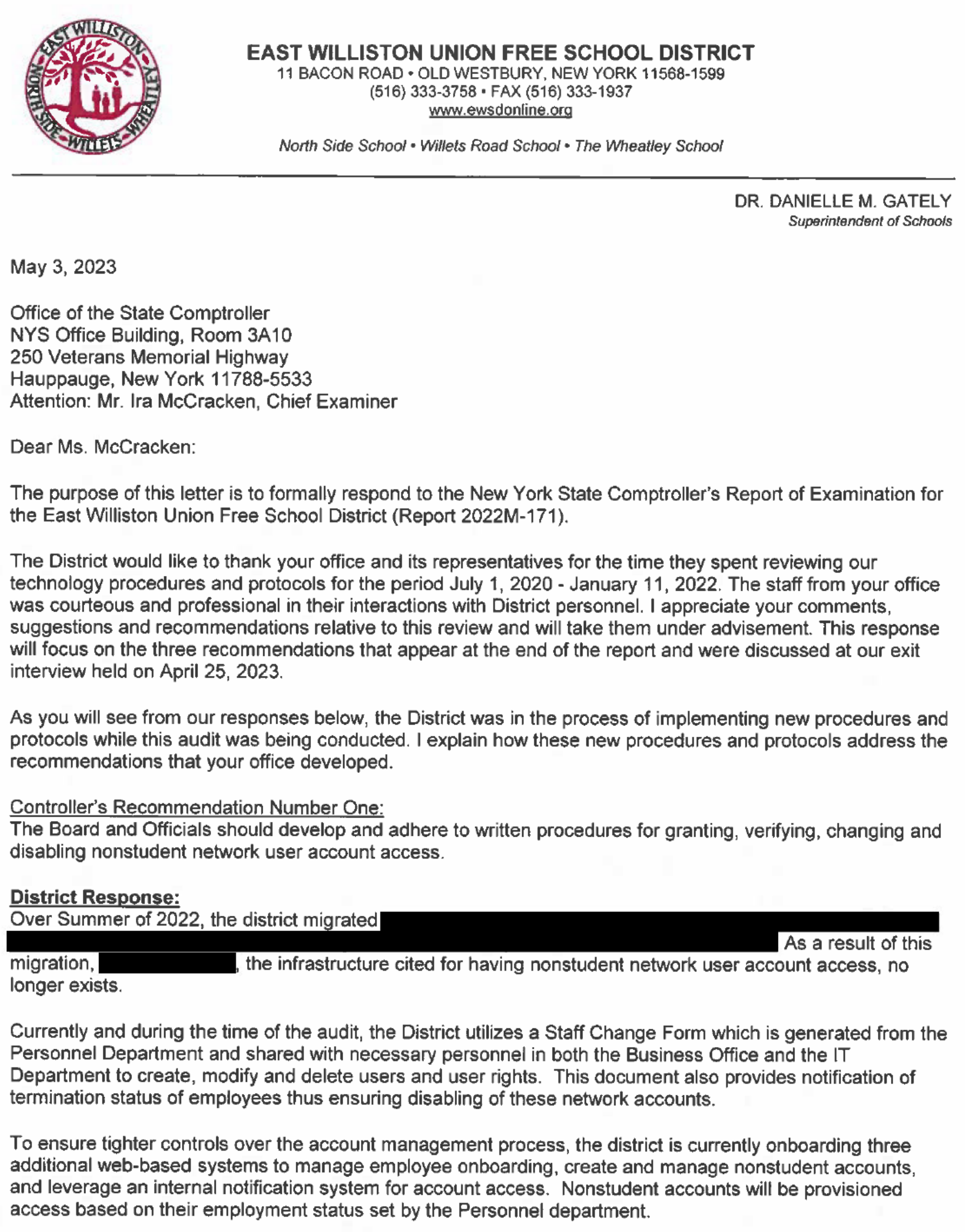
The IT Director should:

2. Disable network user accounts of former employees as soon as they leave District 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.

Appendix A: Response From District Officials

Portions of the District's response were redacted for security concerns.



EAST WILLISTON UNION FREE SCHOOL DISTRICT
11 BACON ROAD • OLD WESTBURY, NEW YORK 11568-1599
(516) 333-3758 • FAX (516) 333-1937
www.ewsdonline.org

North Side School • Willets Road School • The Wheatley School

DR. DANIELLE M. GATELY
Superintendent of Schools

May 3, 2023

Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788-5533
Attention: Mr. Ira McCracken, Chief Examiner

Dear Ms. McCracken:

The purpose of this letter is to formally respond to the New York State Comptroller's Report of Examination for the East Williston Union Free School District (Report 2022M-171).

The District would like to thank your office and its representatives for the time they spent reviewing our technology procedures and protocols for the period July 1, 2020 - January 11, 2022. The staff from your office was courteous and professional in their interactions with District personnel. I appreciate your comments, suggestions and recommendations relative to this review and will take them under advisement. This response will focus on the three recommendations that appear at the end of the report and were discussed at our exit interview held on April 25, 2023.

As you will see from our responses below, the District was in the process of implementing new procedures and protocols while this audit was being conducted. I explain how these new procedures and protocols address the recommendations that your office developed.

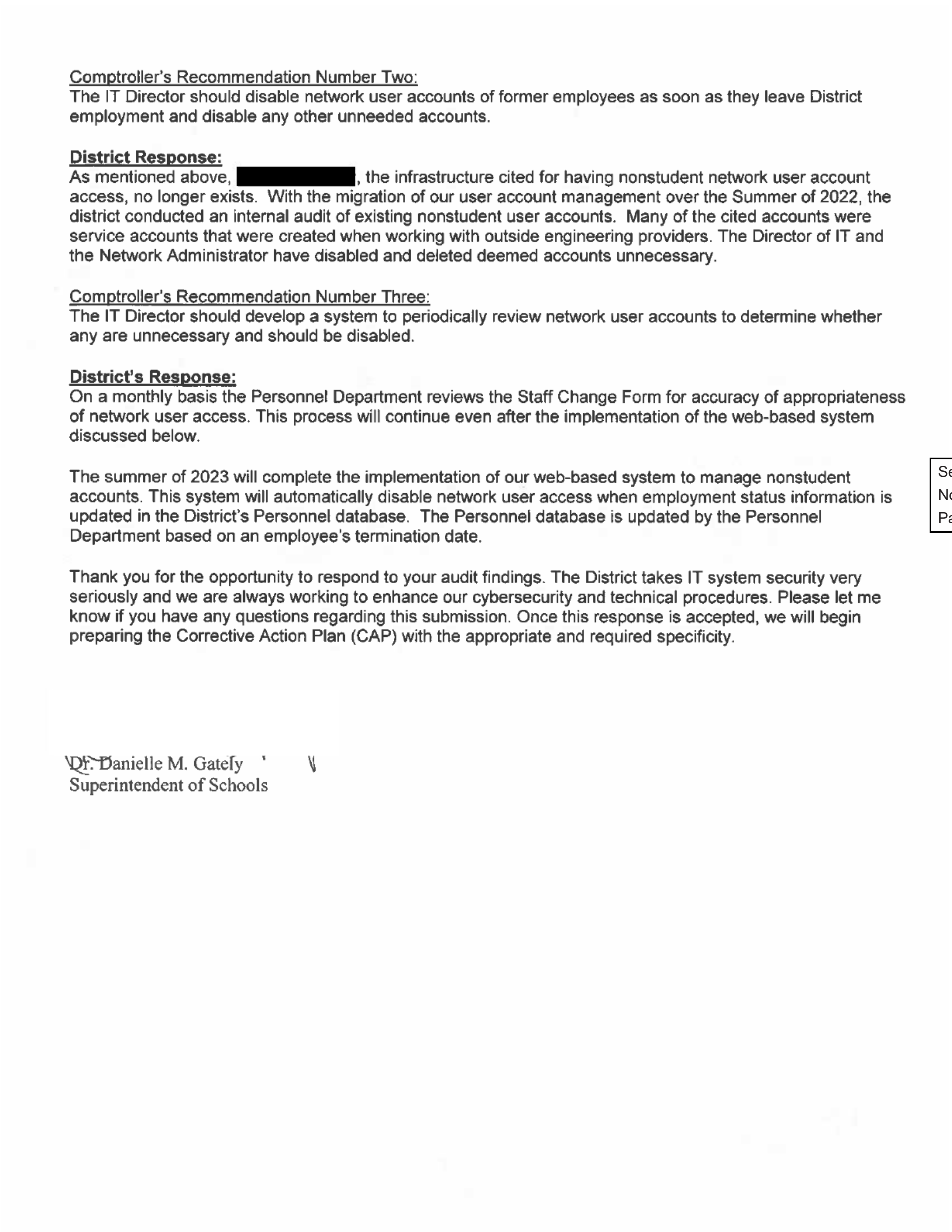
Controller's Recommendation Number One:
The Board and Officials should develop and adhere to written procedures for granting, verifying, changing and disabling nonstudent network user account access.

District Response:
Over Summer of 2022, the district migrated [redacted] As a result of this migration, [redacted], the infrastructure cited for having nonstudent network user account access, no longer exists.

Currently and during the time of the audit, the District utilizes a Staff Change Form which is generated from the Personnel Department and shared with necessary personnel in both the Business Office and the IT Department to create, modify and delete users and user rights. This document also provides notification of termination status of employees thus ensuring disabling of these network accounts.

To ensure tighter controls over the account management process, the district is currently onboarding three additional web-based systems to manage employee onboarding, create and manage nonstudent accounts, and leverage an internal notification system for account access. Nonstudent accounts will be provisioned access based on their employment status set by the Personnel department.

See Note 1 Page 8



Comptroller's Recommendation Number Two:
The IT Director should disable network user accounts of former employees as soon as they leave District employment and disable any other unneeded accounts.

District Response:
As mentioned above, [redacted], the infrastructure cited for having nonstudent network user account access, no longer exists. With the migration of our user account management over the Summer of 2022, the district conducted an internal audit of existing nonstudent user accounts. Many of the cited accounts were service accounts that were created when working with outside engineering providers. The Director of IT and the Network Administrator have disabled and deleted deemed accounts unnecessary.

Comptroller's Recommendation Number Three:
The IT Director should develop a system to periodically review network user accounts to determine whether any are unnecessary and should be disabled.

District's Response:
On a monthly basis the Personnel Department reviews the Staff Change Form for accuracy of appropriateness of network user access. This process will continue even after the implementation of the web-based system discussed below.

The summer of 2023 will complete the implementation of our web-based system to manage nonstudent accounts. This system will automatically disable network user access when employment status information is updated in the District's Personnel database. The Personnel database is updated by the Personnel Department based on an employee's termination date.

See
Note 1
Page 8

Thank you for the opportunity to respond to your audit findings. The District takes IT system security very seriously and we are always working to enhance our cybersecurity and technical procedures. Please let me know if you have any questions regarding this submission. Once this response is accepted, we will begin preparing the Corrective Action Plan (CAP) with the appropriate and required specificity.

Dr. Danielle M. Gately
Superintendent of Schools

Appendix B: OSC Comment on the District’s Response

Note 1

Although the District has indicated their new system will create and manage nonstudent network user accounts based on employment status, this does not address monitoring and management of all network user accounts such as the shared and service network user accounts.

Appendix C: 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 the District's IT policies and procedures and interviewed the IT Director, Assistant Superintendent for Business and BOCES technicians to gain an understanding of the District's IT environment and internal controls related to network user account management and monitoring and to determine whether the policies and procedures were adequate.
- We ran a computerized audit script on December 6, 2021 to examine the District's domain controller.[2] The District has a total of 2,461 enabled network user accounts. We excluded the 1,768 student accounts and examined the 693 nonstudent enabled network user accounts. We compared the enabled network user accounts to a list of current employees and interviewed the IT Director regarding unused and other potentially unneeded accounts to identify unnecessary accounts.
- We reviewed all 262 generic network user accounts and discussed the purpose of each with the IT Director to determine whether they were needed.
- We reviewed the District's staff change log to gain an understanding of their process for documenting, creating and disabling network user accounts.

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 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

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

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 D: Resources and Services

Regional Office Directory
www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/files/local-government/publications/pdf/cyber-security-guide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/local-government/academy

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

www.osc.state.ny.us/local-government

Local Government and School Accountability Help Line: (866) 321-8503

HAUPPAUGE REGIONAL OFFICE – Ira McCracken, Chief of Municipal Audits

NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York 11788-5533

Tel (631) 952-6534 • Fax (631) 952-6091 • Email: Muni-Hauppauge@osc.ny.gov

Serving: Nassau, Suffolk counties