New York State Comptroller
THOMAS P. DiNAPOLI

Hicksville Union Free School District

Managing Network User Accounts

2023M-20 | August 2023

Contents

Report Highlights

Hicksville Union Free School District

Audit Objective

Determine whether Hicksville Union Free School District (District) officials established adequate controls for managing business office network user accounts to help prevent unauthorized computer use, access and loss.

Key Findings

District officials did not properly manage network user account controls to help maintain continuity of business office operations and prevent unauthorized computer use, access and loss. Officials also did not establish written procedures for granting, verifying, changing and disabling network user account access, including business office network user account access.

In addition, sensitive IT control weaknesses were confidentially communicated to District officials.

Key Recommendation

Establish written procedures for granting, verifying, changing and disabling business office network user account access.

District officials generally agreed with our recommendations and have initiated or indicated they plan 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 Oyster Bay in Nassau County, is governed by an elected seven-member Board of Education (Board) responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools is the chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction.

The Assistant Superintendent for Business is responsible for managing business office staff. The Director of Educational Technology (IT Director) is responsible for establishing network user account controls, including those involving business office computers. The District contracted with an outside vendor to provide an IT Manager, five IT technicians and one digital media specialist to monitor and service the network, and provide IT support, including creating, modifying and disabling network user account access, through the District's Help Desk under the IT Director's supervision.

Quick Facts

District Business Office	
Network User Accounts	11
Employees	11
Computers	14
Cost of Third-Party IT Services in 2021-22	$791,831

Audit Period

July 1, 2021 – July 7, 2022

Network User Account Management Controls

What Controls Should Officials Establish To Manage Network User Accounts?

Because user accounts provide access to the network, school district officials should establish controls to 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 user accounts are additional entry points for attackers to attempt to gain unauthorized access and then to potentially use to inappropriately access and view personal, private and sensitive information (PPSI),[1] make changes to official school district records or deny legitimate access to electronic information when needed.

School district officials should establish controls such as written procedures for actively managing user accounts, including granting, verifying, changing and disabling network user account access and regularly monitoring the accounts to ensure they are appropriate and authorized. These written procedures should establish who has the authority to grant or change access (e.g., department manager approval) and document the process for revoking network access by immediately disabling unneeded user accounts when no longer needed.

Officials Did Not Establish Written Procedures for Managing Network User Accounts

The IT Director did not establish written procedures for granting, verifying, changing and disabling network user account access. In the absence of written procedures, we interviewed the IT Director and IT Manager to gain an understanding of how network user account access was granted to new business office employees and disabled when business office employees left the District.

Prior to September 2021, creating an employee network user account involved an employee's supervisor submitting a ticket with the District's Help Desk, and an IT technician would verify that the new user was a District employee with the District's personnel department (personnel) before creating the user account. Personnel would notify the Help Desk to disable network user account access of any employees leaving District employment. Since September 2021, the District used software to help automate the process of creating and disabling network user accounts for all District employees, including business office employees. When business office employees are hired, personnel creates employee records in the District's financial software and upon Board approval of the appointments, marks the employee records as active. The Assistant Superintendent for Business submits a ticket to the Help Desk to modify user

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

rights for business office employee network user accounts. When employees leave the District, personnel marks the employee records as inactive. On a daily basis, the IT Director's secretary (secretary) generates a list of active employees in the financial software. On a nightly basis, the software used to help automate the network user account creation and disabling process automatically compares the secretary's generated list of active employees to a list of enabled network user accounts, and then automatically creates network user accounts for newly activated employees and disables the accounts for employees that are no longer active. The IT Director could not explain why there were no written procedures for granting, verifying, changing and disabling network user account access. The IT Director agreed that written procedures were necessary and said that he began the process of developing procedures as a result of our audit inquiry.

A lack of written procedures for granting, verifying, changing and disabling network user account access increases the risk that IT staff may not have the guidance to properly manage network user account access to help maintain continuity of business office operations and prevent unauthorized computer use, access and loss. This risk is heightened because IT personnel do not periodically review and compare a list of enabled network user accounts to a master employee list. We reviewed all 1,194 employee network user accounts to determine whether there were any unneeded business office network user accounts. We also followed up with the IT Director and the Assistant Superintendent for Business to assess whether enabled network user accounts associated with business office users were needed. Based on our review, we determined that there were no unneeded business office network user accounts. While our review did not identify any unnecessary business office network user accounts, because user accounts were not periodically reviewed to ensure they are still needed, there is an increased risk that errors during the network user account management process could occur and go undetected. Therefore, the risk remains that unneeded network user accounts, such as accounts for former employees, may not be immediately disabled and could remain enabled on the network. If an unneeded account is compromised, an attacker could use it to inappropriately access the District's network. 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 cripple and/or completely shut down the District network;
- 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; and

- Inappropriately accessing and changing District records, such as employee direct deposit information.

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

What Do We Recommend?

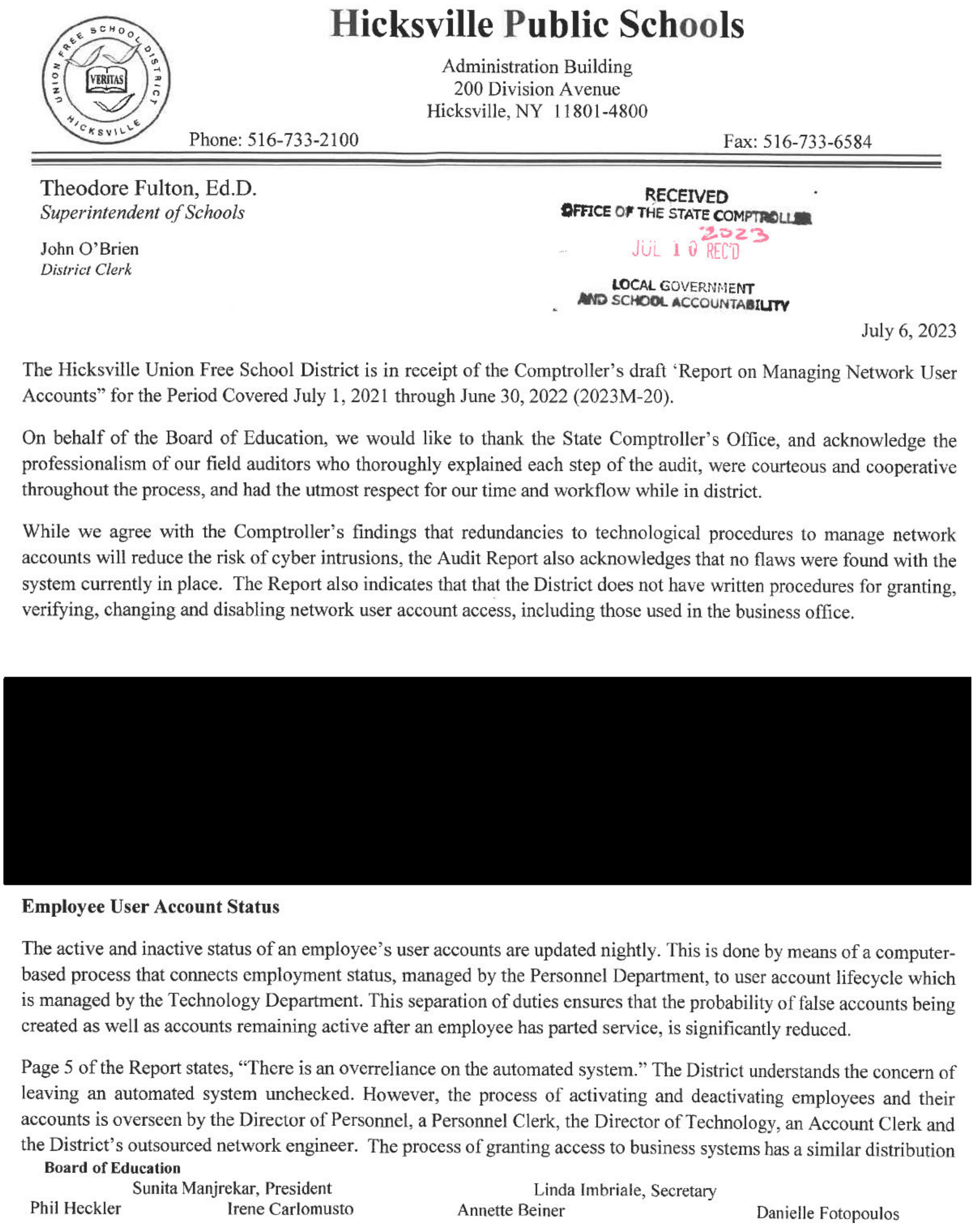
The IT Director should:

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

2. Establish and implement a system to periodically review enabled network user accounts to determine whether they are needed, and promptly disable those that are deemed unneeded.

Appendix A: Response From District Officials

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



Hicksville Public Schools

Administration Building
200 Division Avenue
Hicksville, NY 11801-4800

Phone: 516-733-2100 Fax: 516-733-6584

Theodore Fulton, Ed.D.
Superintendent of Schools

John O'Brien
District Clerk

July 6, 2023

The Hicksville Union Free School District is in receipt of the Comptroller's draft 'Report on Managing Network User Accounts" for the Period Covered July 1, 2021 through June 30, 2022 (2023M-20).

On behalf of the Board of Education, we would like to thank the State Comptroller's Office, and acknowledge the professionalism of our field auditors who thoroughly explained each step of the audit, were courteous and cooperative throughout the process, and had the utmost respect for our time and workflow while in district.

While we agree with the Comptroller's findings that redundancies to technological procedures to manage network accounts will reduce the risk of cyber intrusions, the Audit Report also acknowledges that no flaws were found with the system currently in place. The Report also indicates that that the District does not have written procedures for granting, verifying, changing and disabling network user account access, including those used in the business office.

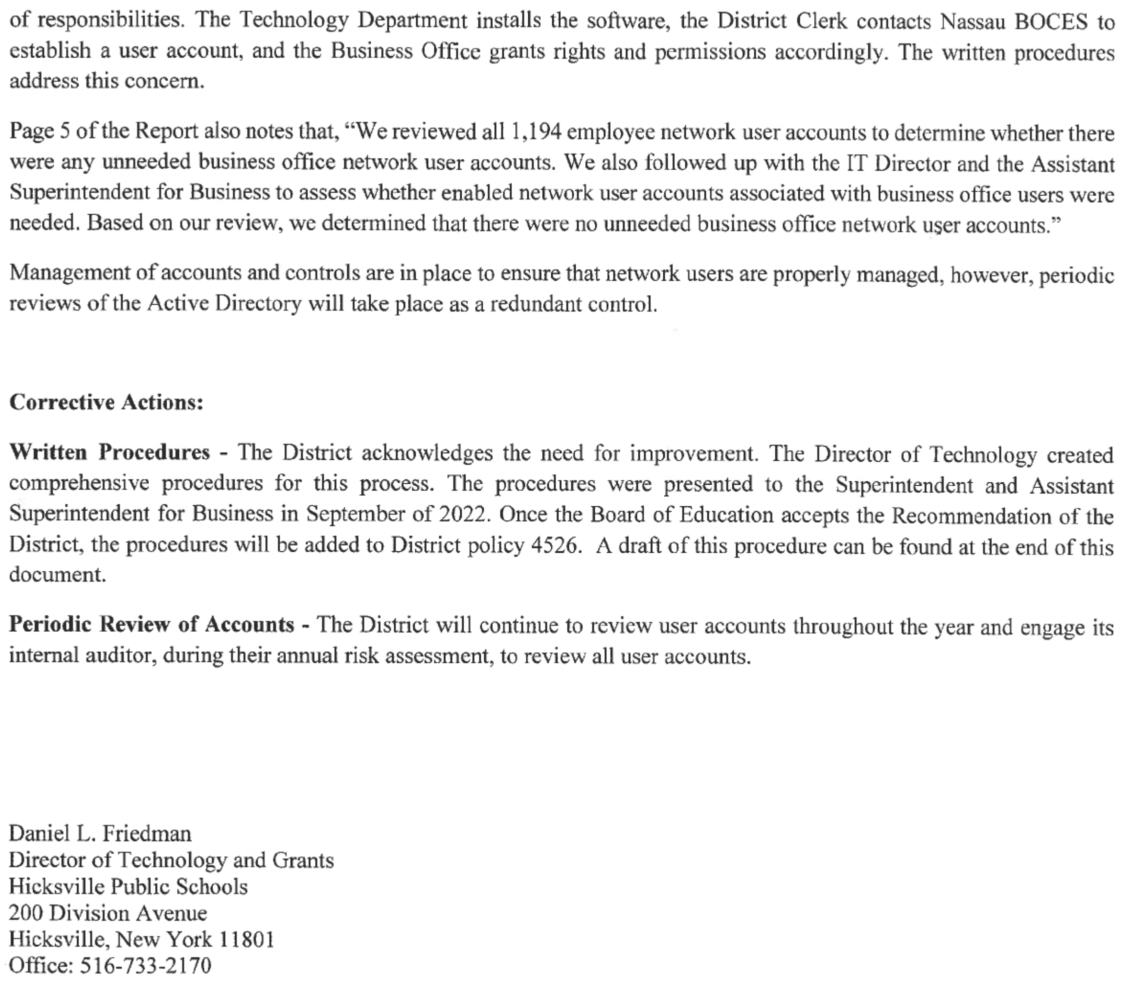
See
Note 1
Page 8

[redacted]

Employee User Account Status

The active and inactive status of an employee's user accounts are updated nightly. This is done by means of a computer-based process that connects employment status, managed by the Personnel Department, to user account lifecycle which is managed by the Technology Department. This separation of duties ensures that the probability of false accounts being created as well as accounts remaining active after an employee has parted service, is significantly reduced.

Page 5 of the Report states, "There is an overreliance on the automated system." The District understands the concern of leaving an automated system unchecked. However, the process of activating and deactivating employees and their accounts is overseen by the Director of Personnel, a Personnel Clerk, the Director of Technology, an Account Clerk and the District's outsourced network engineer. The process of granting access to business systems has a similar distribution



of responsibilities. The Technology Department installs the software, the District Clerk contacts Nassau BOCES to establish a user account, and the Business Office grants rights and permissions accordingly. The written procedures address this concern.

Page 5 of the Report also notes that, "We reviewed all 1,194 employee network user accounts to determine whether there were any unneeded business office network user accounts. We also followed up with the IT Director and the Assistant Superintendent for Business to assess whether enabled network user accounts associated with business office users were needed. Based on our review, we determined that there were no unneeded business office network user accounts."

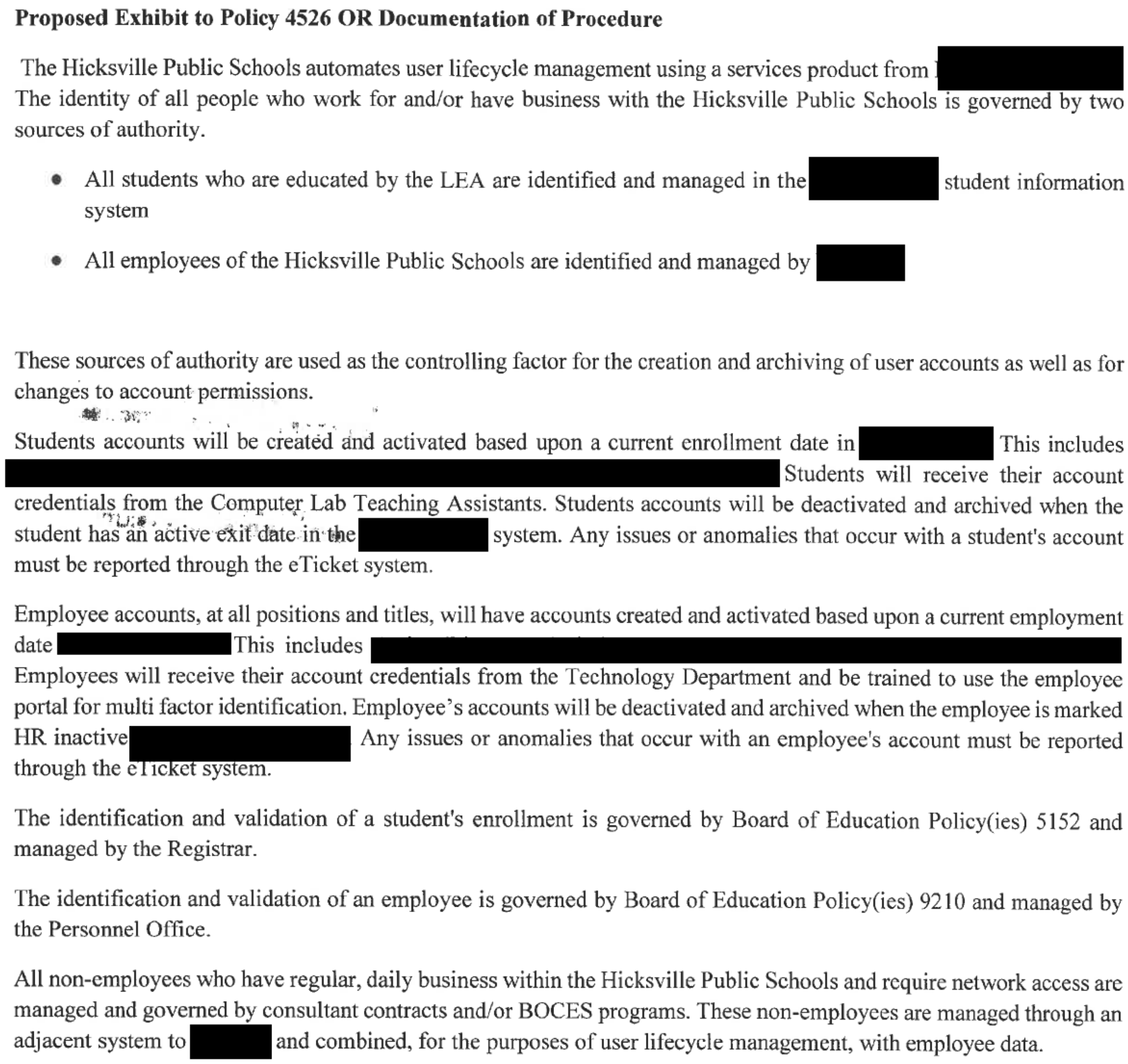
Management of accounts and controls are in place to ensure that network users are properly managed, however, periodic reviews of the Active Directory will take place as a redundant control.

Corrective Actions:

Written Procedures - The District acknowledges the need for improvement. The Director of Technology created comprehensive procedures for this process. The procedures were presented to the Superintendent and Assistant Superintendent for Business in September of 2022. Once the Board of Education accepts the Recommendation of the District, the procedures will be added to District policy 4526. A draft of this procedure can be found at the end of this document.

Periodic Review of Accounts - The District will continue to review user accounts throughout the year and engage its internal auditor, during their annual risk assessment, to review all user accounts.

Daniel L. Friedman
Director of Technology and Grants
Hicksville Public Schools
200 Division Avenue
Hicksville, New York 11801
Office: 516-733-2170



Proposed Exhibit to Policy 4526 OR Documentation of Procedure

The Hicksville Public Schools automates user lifecycle management using a services product from [redacted] The identity of all people who work for and/or have business with the Hicksville Public Schools is governed by two sources of authority.

- All students who are educated by the LEA are identified and managed in the [redacted] student information system
- All employees of the Hicksville Public Schools are identified and managed by [redacted]

These sources of authority are used as the controlling factor for the creation and archiving of user accounts as well as for changes to account permissions.

Students accounts will be created and activated based upon a current enrollment date in [redacted] This includes [redacted] Students will receive their account credentials from the Computer Lab Teaching Assistants. Students accounts will be deactivated and archived when the student has an active exit date in the [redacted] system. Any issues or anomalies that occur with a student's account must be reported through the eTicket system.

Employee accounts, at all positions and titles, will have accounts created and activated based upon a current employment date [redacted] This includes [redacted] Employees will receive their account credentials from the Technology Department and be trained to use the employee portal for multi factor identification. Employee's accounts will be deactivated and archived when the employee is marked HR inactive [redacted]. Any issues or anomalies that occur with an employee's account must be reported through the eTicket system.

The identification and validation of a student's enrollment is governed by Board of Education Policy(ies) 5152 and managed by the Registrar.

The identification and validation of an employee is governed by Board of Education Policy(ies) 9210 and managed by the Personnel Office.

All non-employees who have regular, daily business within the Hicksville Public Schools and require network access are managed and governed by consultant contracts and/or BOCES programs. These non-employees are managed through an adjacent system to [redacted] and combined, for the purposes of user lifecycle management, with employee data.

Appendix B: OSC Comment on the District's Response

Note 1

The audit report does not acknowledge that no flaws were found with the system currently in place. The report indicates that the management of network user accounts should include regularly monitoring the accounts to ensure they are appropriate and authorized, and immediately disabling unneeded user accounts when no longer needed. Because no one at the District is periodically reviewing and comparing a list of enabled network user accounts to a master employee list, the risk remains that unneeded network user accounts, such as accounts for former employees, may not be immediately disabled.

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 and IT Manager to gain an understanding of network user account controls established to help prevent unauthorized business office computer use, access and loss.
- We ran a computerized audit script on the District's domain controller on July 7, 2022 to gather network user account information. We compared the District's 1,194 enabled employee network user accounts to the active employee list to identify whether there were any user accounts for former business office employees and consultants that may be unneeded. We followed up with the IT Director and the Assistant Superintendent for Business to assess whether network user accounts associated with business office users were needed.

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 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.

Serving: Nassau, Suffolk counties