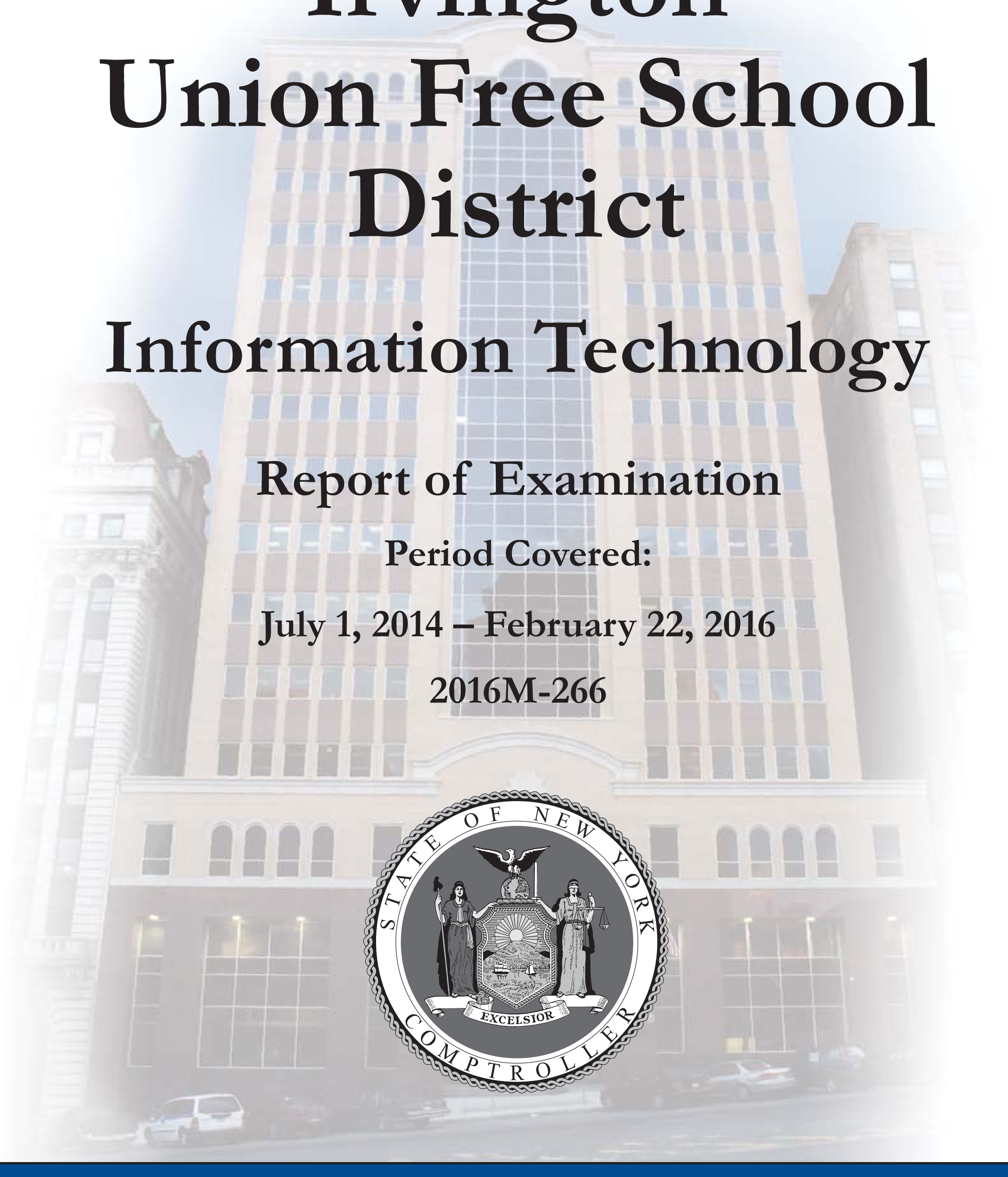
Office of the New York State Comptroller

Division of Local Government
& School Accountability



Irvington Union Free School District

Information Technology

Report of Examination

Period Covered:

July 1, 2014 – February 22, 2016

2016M-266

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

November 2016

Dear School District Officials:

A top priority of the Office of the State Comptroller is to help school district officials manage their districts efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support district operations. The Comptroller oversees the fiscal affairs of districts statewide, as well as districts' compliance with relevant statutes and observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving district operations and Board of Education governance. Audits also can identify strategies to reduce district costs and to strengthen controls intended to safeguard district assets.

Following is a report of our audit of the Irvington Union Free School District, entitled Information Technology. This audit was conducted 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.

This audit's results and recommendations are resources for district officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

Office of the State Comptroller
Division of Local Government
and School Accountability

Introduction

Background

The Irvington Union Free School District (District) is located in the Towns of Greenburgh and Tarrytown and in the Village of Irvington in Westchester County. The District is governed by the Board of Education (Board), which is composed of five elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools is the District's 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 District operates four schools with approximately 1,700 students and 315 employees. Budgeted appropriations for the 2015-16 fiscal year were approximately $57.7 million, funded primarily with real property taxes, other tax items and State aid.

The District uses network and web resources to support business operations, such as maintaining financial records; maintaining student records, including personal, private and sensitive information; performing online banking transactions; and communicating. The Technology Director oversees the technology department and makes decisions about hardware and application acquisitions or changes. The District contracts with the Lower Hudson Regional Information Center for some information technology (IT) services.

Objective

The objective of our audit was to examine internal controls over IT. Our audit addressed the following related question:

- Are internal controls over IT appropriately designed and operating effectively to adequately safeguard District data?

Scope and Methodology

We examined internal controls over the District's IT for the period July 1, 2014 through February 22, 2016. We extended our scope to the end of fieldwork, June 10, 2016, to complete computer testing. Our audit also examined the adequacy of certain 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 our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit are included in Appendix B of this report. 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.

Comments of District Officials and Corrective Action

The results of our audit and recommendations have been discussed with District officials, and their comments, which appear in Appendix A, have been considered in preparing this report. District officials generally agreed with our recommendations and indicated they planned to initiate corrective action.

The Board has the responsibility to initiate corrective action. 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, 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, with a copy forwarded to 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 Board should make the CAP available for public review in the District Clerk's office.

Information Technology

The use of IT affects the fundamental manner in which transactions are initiated, recorded, processed and reported. The extent to which computer processing is used in student database applications, and the complexity of that processing, determines the specific risks that IT poses to the District's internal controls. The District's widespread use of IT presents a number of internal control risks that must be addressed. Those risks include unauthorized access to data, unauthorized changes to data in master files and loss of data. District officials must therefore develop an acceptable use policy and an email policy and install and configure web filtering software and virus protection software to safeguard data from loss or misuse.

The Board needs to improve internal controls to effectively protect the District's computer system and data. The Board has developed an acceptable use policy and an email policy. However, the acceptable use policy does not address computer users who do not use the District's computers for instructional purposes or the inappropriate use of IT equipment. In addition, the email policy allows for the use of personal email through external mail servers. Further, District staff are able to access websites such as online shopping, social networking, travel and automobile sites that are unrelated to their District duties and violate the acceptable use policy because the District's web filtering software is not configured to block access. We also found that one District computer had no virus protection software installed. As a result, users could expose the District to malicious attacks that could compromise systems and data. Further, time spent by employees using District resources for personal reasons represents lost District resources.

Policies

Policies over IT provide criteria and guidance for computer-related operations. Effective protection includes the adoption of an acceptable use policy that informs users about the appropriate and safe use of District computers and an email policy to ensure security scanning at more than one point. The Board should periodically review and update these policies to reflect changes in technology or the computing environment. Computer users need to be aware of security risks and be properly trained in practices that reduce the internal and external threats to the network.

The District has an acceptable use policy and an email policy. However, the acceptable use policy does not address computer users who do not use the District's computers for instructional purposes, what constitutes appropriate and inappropriate use of IT equipment, the Board's expectations concerning the personal use of IT equipment or user privacy. Further, although the Board has adopted an email policy that outlines acceptable use of email in the District, the policy allows the use of personal email through external mail servers.

Consequently, there is no requirement for the Internet and computers to be used in an appropriate and secure manner and email users can circumvent the multiple point security controls that protect the District's systems and data. As a result, users could expose the District to malicious attacks that could compromise systems and data by putting computers at risk for viruses or malicious software (malware).[1]

Internet Use

Many school districts find that the Internet is a nearly indispensable resource for conducting business. However, users are susceptible to significant threats from cyber criminals who exploit the vulnerabilities of IT systems to gain unauthorized access to sensitive data. For example, computers can be infected by malware that can install a keystroke logger that captures identification and password information. Internet browsing increases the likelihood that users will be exposed to malware that may compromise data confidentiality. District officials can reduce the risks to sensitive data and IT assets by monitoring Internet usage and using web filtering software to block access to unacceptable websites and limit access to those sites that comply with the acceptable use policy.

We selected and reviewed a judgmental sample of 20 District computers[2] that included 57 user profiles.[3] District staff were able to access websites such as online shopping, social networking, travel and automobile sites that were unrelated to their District duties and violated the District's acceptable use policy. Although there are business reasons to access a shopping site, only business-related shopping sites should be permitted and only those responsible for purchasing should be permitted to access those sites. In addition, District employees were able to access their personal email accounts through external mail servers.

This occurred because District officials did not sufficiently monitor Internet usage or configure the web filtering software to block access to these sites. Inappropriate use of District computers could potentially expose the District to virus attacks or compromise systems and data, including key financial and confidential information. Further, time spent by employees using District resources for personal reasons while they are supposed to be working represents lost District resources.

[1] Malware infiltrates a computer system by circumventing network defenses, avoiding detection and resisting efforts to disable it.

[2] We selected all five of the Business Office computers and 15 of the 21 computers in the special education department.

[3] Some of the computers included multiple profiles of web history depending on the number of users. The total number of profiles, excluding IT staff and default users, was 392.

Antivirus Software

Malicious software, or malware, is designed to harm computer systems. These programs can wreak havoc on systems and electronic data by deleting files, gathering sensitive information such as passwords without the user's knowledge and making systems inoperable. Computer users can inadvertently install malware on their computers in many ways, including opening email attachments, downloading content from the Internet or visiting infected websites. Antivirus software can detect and stop some forms of malware. Antivirus software should be installed and kept current with signature (a set of characteristics also referred to as virus definitions) and software updates. Antivirus definitions should be updated daily and the software should be set to scan for threats throughout the day.

We examined 20 computers and found that 18 had the Districtwide virus protection installed, were receiving daily updates and were set up to scan throughout the day. However, two of these computers did not have the Districtwide virus protection installed. One of the computers had a different virus protection software installed although it was receiving the proper definition updates and was set up to scan throughout the day. The other computer had no virus protection and therefore was not receiving definition updates for any antivirus software or scanning.

Viruses can corrupt data and make computers inoperable. Damage caused by viruses can be expensive to fix and can cause significant losses in productivity until corrected. If computers are not properly protected with antivirus and malware software, the District's computer network is at risk of being compromised.

Recommendations

The Board should:

1. Update the District's acceptable use policy to address users who do not use computers for instructional purposes, what constitutes appropriate and inappropriate use of IT equipment, the Board's expectations concerning personal use of IT equipment and user privacy.

2. Consider the risk of allowing users to access personal email through external mail servers and amend the email policy accordingly.

District officials should:

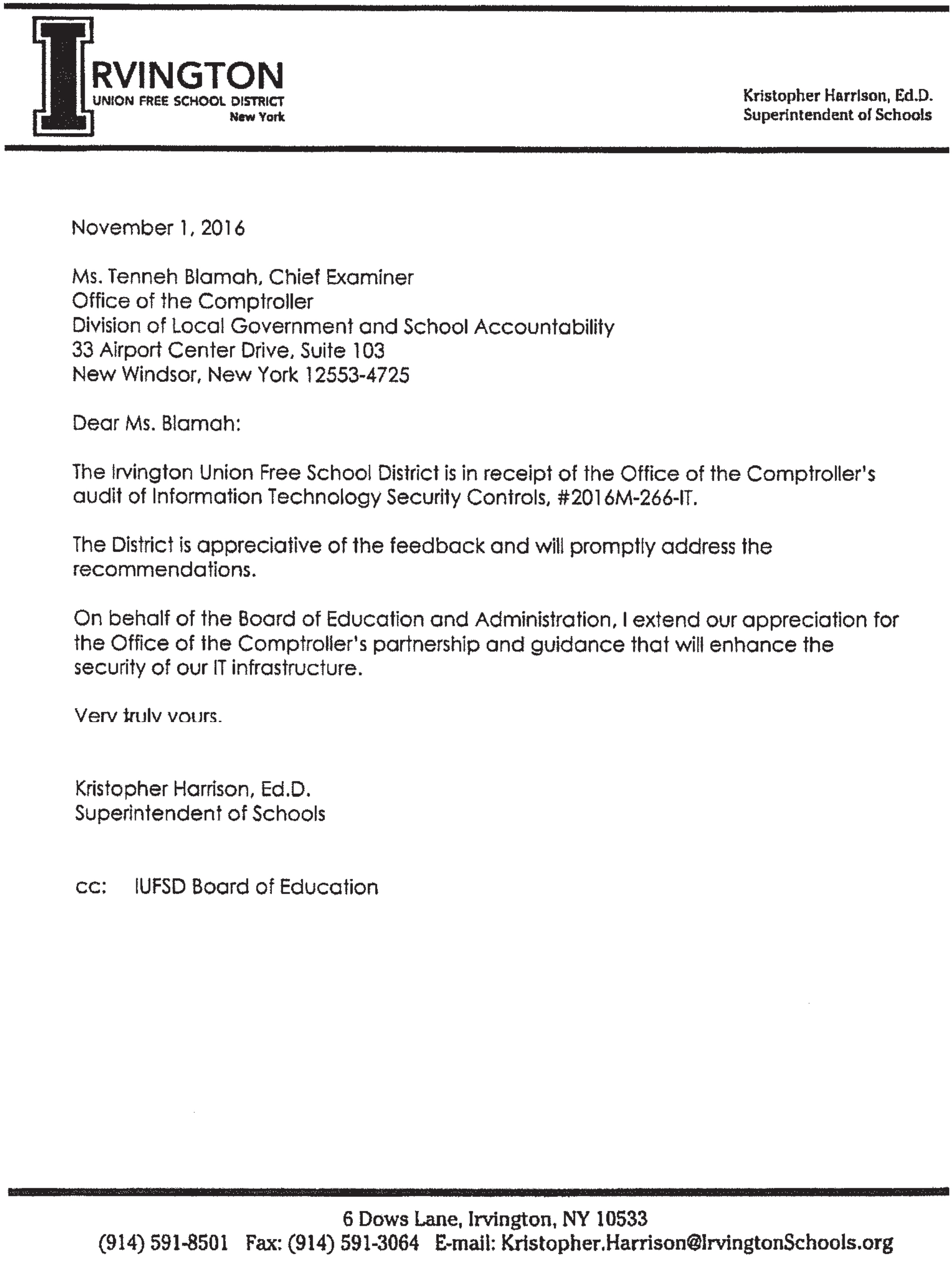
3. Monitor Internet usage and configure the web filtering software to block access to sites that violate the acceptable use policy.

4. Periodically review computers to ensure the designated Districtwide antivirus software is installed and that the computers are receiving definition updates.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

The District officials' response to this audit can be found on the following page.



IRVINGTON
UNION FREE SCHOOL DISTRICT
New York

Kristopher Harrison, Ed.D.
Superintendent of Schools

November 1, 2016

Ms. Tenneh Blamah, Chief Examiner
Office of the Comptroller
Division of Local Government and School Accountability
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725

Dear Ms. Blamah:

The Irvington Union Free School District is in receipt of the Office of the Comptroller's audit of Information Technology Security Controls, #2016M-266-IT.

The District is appreciative of the feedback and will promptly address the recommendations.

On behalf of the Board of Education and Administration, I extend our appreciation for the Office of the Comptroller's partnership and guidance that will enhance the security of our IT infrastructure.

Very truly yours.

Kristopher Harrison, Ed.D.
Superintendent of Schools

cc: IUFSD Board of Education

6 Dows Lane, Irvington, NY 10533
(914) 591-8501 Fax: (914) 591-3064 E-mail: Kristopher.Harrison@IrvingtonSchools.org

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

To achieve our audit objective and obtain valid evidence, we performed the following procedures:

- We reviewed the District's policy and procedure manuals to identify IT-related policies and evaluated those policies to gain an understanding of internal controls over IT.

- We interviewed officials and personnel to gain an understanding of internal controls over IT.

- We selected and examined 20 computers by running audit software and examined specific activities on those computers, such as Internet history.

- We reviewed web activity reports for accessed websites that violated the District's acceptable use policy or could put the District's network at risk.

- We selected 20 computers and reviewed their software inventory looking for virus protection software and definition updates. We selected five computers (those assigned to the Treasurer, payroll clerk, accounts payable clerk, Assistant Superintendent for Business and secretary to the Assistant Superintendent for Business) because the officials' duties and privileges involved using and transmitting important electronic data. We selected 15 other computers because their primary users (special education staff) regularly used the individualized education plan application, which contained personal, private and sensitive information. We selected the 15 computers by using a spreadsheet random number generator to select half of the special education staff from each building.

We conducted this performance audit in accordance with 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.

APPENDIX C

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller
Public Information Office
110 State Street, 15th Floor
Albany, New York 12236
(518) 474-4015
http://www.osc.state.ny.us/localgov/

APPENDIX D

OFFICE OF THE STATE COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY

Andrew A. SanFilippo, Executive Deputy Comptroller
Gabriel F. Deyo, Deputy Comptroller
Tracey Hitchen Boyd, Assistant Comptroller

LOCAL REGIONAL OFFICE LISTING

BINGHAMTON REGIONAL OFFICE
H. Todd Eames, Chief Examiner
Office of the State Comptroller
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313
Email: Muni-Binghamton@osc.state.ny.us

Serving: Broome, Chenango, Cortland, Delaware,
Otsego, Schoharie, Sullivan, Tioga, Tompkins Counties

BUFFALO REGIONAL OFFICE
Jeffrey D. Mazula, Chief Examiner
Office of the State Comptroller
295 Main Street, Suite 1032
Buffalo, New York 14203-2510
(716) 847-3647 Fax (716) 847-3643
Email: Muni-Buffalo@osc.state.ny.us

Serving: Allegany, Cattaraugus, Chautauqua, Erie,
Genesee, Niagara, Orleans, Wyoming Counties

GLENS FALLS REGIONAL OFFICE
Jeffrey P. Leonard, Chief Examiner
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, New York 12801-4396
(518) 793-0057 Fax (518) 793-5797
Email: Muni-GlensFalls@osc.state.ny.us

Serving: Albany, Clinton, Essex, Franklin,
Fulton, Hamilton, Montgomery, Rensselaer,
Saratoga, Schenectady, Warren, Washington Counties

HAUPPAUGE REGIONAL OFFICE
Ira McCracken, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788-5533
(631) 952-6534 Fax (631) 952-6530
Email: Muni-Hauppauge@osc.state.ny.us

Serving: Nassau and Suffolk Counties

NEWBURGH REGIONAL OFFICE
Tenneh Blamah, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725
(845) 567-0858 Fax (845) 567-0080
Email: Muni-Newburgh@osc.state.ny.us

Serving: Columbia, Dutchess, Greene, Orange,
Putnam, Rockland, Ulster, Westchester Counties

ROCHESTER REGIONAL OFFICE
Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street, Suite 522
Rochester, New York 14614-1608
(585) 454-2460 Fax (585) 454-3545
Email: Muni-Rochester@osc.state.ny.us

Serving: Cayuga, Chemung, Livingston, Monroe,
Ontario, Schuyler, Seneca, Steuben, Wayne, Yates Counties

SYRACUSE REGIONAL OFFICE
Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428
(315) 428-4192 Fax (315) 426-2119
Email: Muni-Syracuse@osc.state.ny.us

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

STATEWIDE AUDITS
Ann C. Singer, Chief Examiner
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313