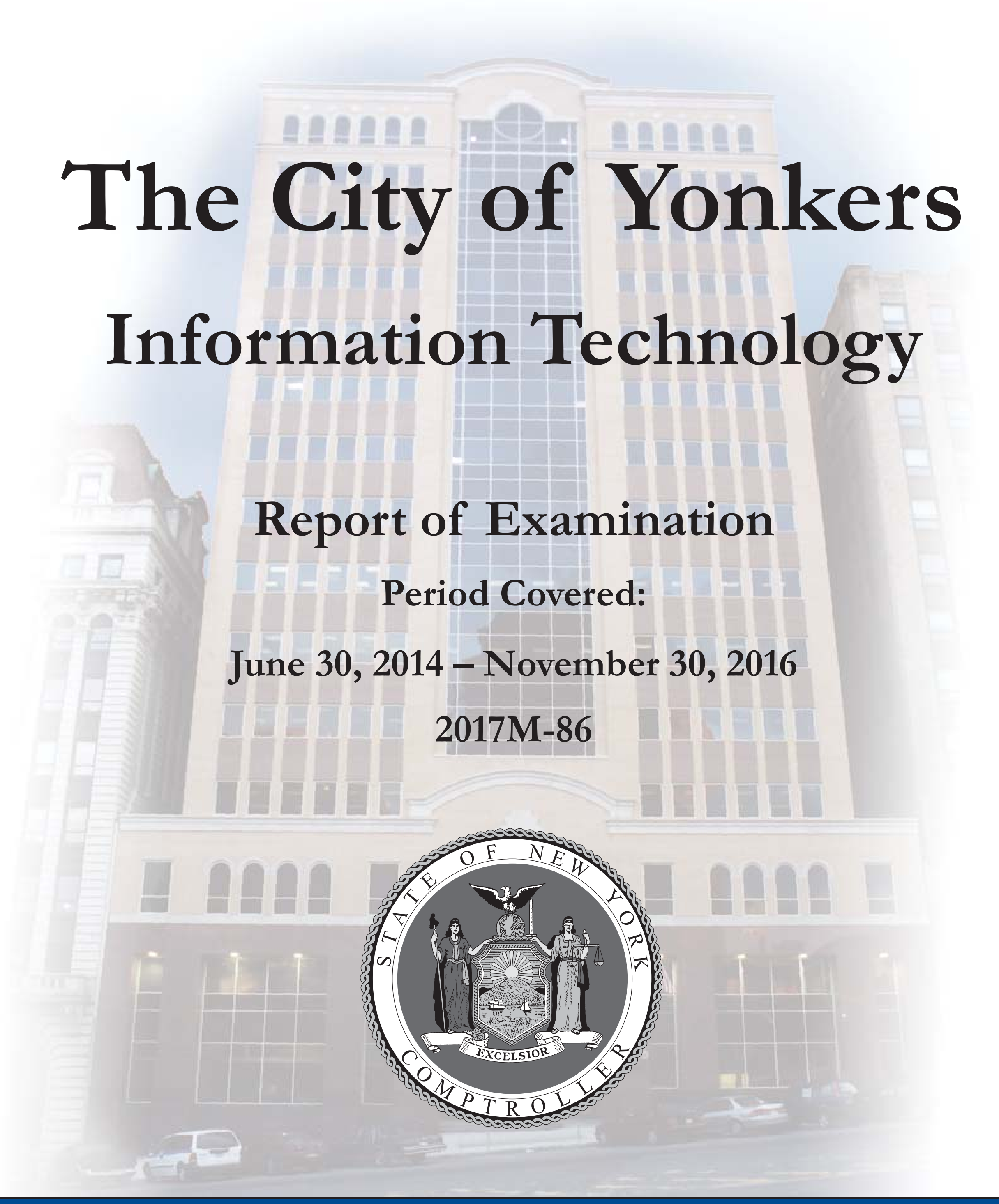
Office of the New York State Comptroller

Division of Local Government
& School Accountability



The City of Yonkers

Information Technology

Report of Examination

Period Covered:

June 30, 2014 – November 30, 2016

2017M-86

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

August 2017

Dear City Officials:

A top priority of the Office of the State Comptroller is to help local government officials manage government resources efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support government operations. The Comptroller oversees the fiscal affairs of local governments statewide, as well as 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 operations and City Council governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard government assets.

Following is a report of our audit of the City of Yonkers, 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 local 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

State of New York
Office of the State Comptroller

EXECUTIVE SUMMARY

The City of Yonkers (City) is the fourth largest city in New York State. An elected seven-member City Council is the City's legislative branch. The Mayor is the chief executive officer and is responsible, along with other administrative staff, for the City's day-to-day for administration. The Commissioner of Finance is the chief fiscal officer and is responsible for the oversight and accountability of financial activities. The Commissioner of Information is responsible for the oversight and accountability of information technology (IT) activities. Yonkers Public Schools (YPS) is a component unit of the City. Educational activities are governed by the Board of Education. YPS financial activities are handled by the City.

The City's 2016-17 budget was approximately $1.1 billion, funded primarily by real property taxes, sales tax, a City income tax and State aid. The City has approximately 3,000 full- and part-time employees, including 43 City and YPS Department of Information Technology (IT department) employees. The IT department's adopted 2016-17 budget was approximately $11.6 million ($7.2 million for City activities and $4.4 million for YPS operations).

Scope and Objective

The objective of our audit was to determine whether City officials established adequate internal controls over IT assets for the period June 30, 2014 through November 30, 2016. Our audit addressed the following related question:

- Did City officials provide adequate oversight of IT assets and ensure that IT systems were adequately secured and protected against unauthorized access and loss?

Audit Results

City officials need to improve internal controls over IT assets to help ensure that IT systems are sufficiently secured and protected against unauthorized access and loss. The IT department's acceptable computer use policy was not signed or acknowledged by all employees. City officials have also not classified personal, private and sensitive information (PPSI) based on its level of sensitivity and the potential impact should that data be disclosed, altered or destroyed without authorization. In addition, City officials did not ensure that employees received adequate cyber security training and have not adopted a breach notification policy or a disaster recovery plan.

IT department officials did not maintain accurate and up-to-date IT hardware inventory records and were unable to locate 140 items listed on the City's inventory.[1] We also identified significant weaknesses in the use of web filters. Our review of web histories on 26 computers[2] disclosed that City employees were able to access websites unrelated to City activities, such as personal online brokerage and trading, personal email and social media. We also found deficiencies in online banking activities to protect the City's financial assets because City officials did not adopt a written policy addressing electronic banking transactions, develop specific written procedures for electronic transfers, provide adequate monitoring of online bank account activities or implement appropriate online banking security controls and alerts. As a result, the City's IT software, hardware and data was not adequately protected from loss or misuse due to errors, malicious intent and accidents.

Comments of City Officials

The results of our audit and recommendations have been discussed with City officials, and their comments, which appear in Appendix A, have been considered in preparing this report. City officials generally agreed with our recommendations and indicated they planned to take corrective action. Appendix B includes our comment on an issue raised in the City's response letter.

[1] City officials were unable to provide information on the value of these items.

[2] See Appendix B for information on our methodology.

Introduction

Background

The City of Yonkers (City) is the fourth largest city in New York State with a population of more than 200,000. An elected seven-member City Council (Council) is the City's legislative branch. The Mayor is the chief executive officer and is responsible, along with other administrative staff, for the City's day-to-day administration. The Commissioner of Finance is the City's chief fiscal officer and is responsible for the oversight and accountability of financial activities. The Commissioner of Information is responsible for the oversight and accountability for the City's Information Technology (IT) activities and resources. Yonkers Public Schools (YPS) is a component unit of the City. Educational activities are governed by the Board of Education. YPS financial activities are handled by the City.

The City's 2016-17 budget was approximately $1.1 billion, funded primarily by real property taxes, sales tax, a City income tax and State aid. The City employs approximately 3,000 employees, who are assigned to departments that provide services including general government support, road maintenance, snow removal, water and sewer services and public safety. The IT department's adopted 2016-17 budget was approximately $11.6 million ($7.2 million for City activities and $4.4 million for YPS operations) with 43 employees.

Objective

The objective of our audit was to determine whether City officials established adequate internal controls over IT assets. Our audit addressed the following related question:

- Did City officials provide adequate oversight of IT assets and ensure that IT systems were adequately secured and protected against unauthorized access and loss?

Scope and Methodology

We examined the City's controls over IT for the period June 30, 2014 through November 30, 2016. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to City officials.

Except for the independence impairment discussed in the next paragraph, 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 relevant population size and the sample selected for examination.

Pursuant to the Fiscal Agent Act (Chapter 488 of the Laws of 1976), the Office of the State Comptroller (OSC) maintains City assets in a special debt service fund bank account, invests those funds on behalf of and at the direction of the City, and makes payments on behalf of the City for any debt service payments due. We believe that independence concerns are mitigated as City officials oversee the required services performed by OSC under the Fiscal Agent Act and evaluate the results of the services performed. However, GAGAS explicitly states that these services impair an external auditor's independence with respect to an audited entity.[3]

Comments of City Officials and Corrective Action

The results of our audit and recommendations have been discussed with City officials, and their comments, which appear in Appendix A, have been considered in preparing this report. City officials generally agreed with our recommendations and indicated they planned to take corrective action. Appendix B includes our comment on an issue raised in the City's response letter.

The City Council has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and forwarded to our office within 90 days, pursuant to Section 35 of the General Municipal Law. 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. We encourage the Council to make this plan available for public review in the City Clerk's office.

[3] *Government Auditing Standards*, 2011 Revision, paragraph 3.58

Information Technology

The City uses IT to initiate, process, record and report transactions. It also relies on its IT systems for internet access, email and the maintenance of financial and personnel records. Therefore, the IT systems and data are valuable City resources. If IT systems are compromised, the results could range from an inconvenience to a catastrophe and could require extensive effort and resources to evaluate and repair.

City officials are responsible for designing internal controls over the IT environment and resources. Such controls include developing and implementing policies and procedures designed to protect software, hardware and data from loss or misuse due to errors, malicious intent and accidents. Additionally, City officials must ensure that computer assets are physically secured and tracked by maintaining comprehensive, accurate inventory records that are periodically reviewed and updated.

City officials need to improve internal controls over IT assets to help ensure that IT systems are sufficiently secured and protected against unauthorized access and loss. The IT department's acceptable computer use policy was not signed or acknowledged by all employees. City officials have also not classified personal, private and sensitive information (PPSI) based on its level of sensitivity and the potential impact should that data be disclosed, altered or destroyed without authorization. In addition, City officials have not ensured that employees received adequate cyber security training and have not adopted a breach notification policy or a disaster recovery plan. IT department officials did not maintain accurate and up-to-date IT inventory records and were unable to locate 140 items listed on the City's inventory.

We also identified significant weaknesses in the use of web filters. As a result, City employees were able to access websites unrelated to City activities, such as personal online brokerage and trading, personal email and social media. Further, we found deficiencies in the City's online banking activities to protect financial assets because City officials did not adopt a written policy addressing electronic banking transactions, develop specific written procedures for electronic transfers, provide adequate monitoring of online bank account activities or implement appropriate online banking security controls and alerts.

Policies and Procedures

Effective policies and procedures over IT operations provide criteria and guidance for the City's computer related operations and help protect computing resources and data. Effective policies and procedures should include:

- An acceptable use policy that informs employees about appropriate and safe use of City computers.
- Guidelines for collecting, storing and classifying PPSI.
- A requirement for cyber security training so employees who use and manage IT assets understand IT security policies and procedures and their roles and responsibilities related to IT security.
- A breach notification policy that specifies how officials would notify residents whose PPSI was or is reasonably believed to have been acquired by a person without valid authorization.
- A disaster recovery plan with guidance for minimizing loss and restoring operations should a disaster occur.

Once adopted, the City officials need to periodically review and update these policies and procedures as necessary to reflect changes in technology or the City's 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.

City officials have not established adequate policies and procedures to effectively protect the City's IT resources and data. City officials need to improve internal controls by addressing the following areas:

Acceptable Use — The City has an acceptable computer use policy, which was last updated in April 2013. While the policy requires employees to sign an acknowledgement indicating they have read and accept the policy, this has not been enforced. We reviewed personnel records for 29 employees to determine whether they signed the acknowledgment and found that six (21 percent) did not have a signed acknowledgement on file. As a result, all employees may not be aware of the City's acceptable use policy, which increases the risk of exposing the City's IT systems and data to loss or misuse.

Data Classification — In the normal course of business, the City collects and stores data received from residents and those it does business with, including PPSI. Therefore, it is important City officials develop and implement written policy and procedures requiring the data to be classified based on its level of sensitivity and the potential impact should that data be disclosed, altered or destroyed without authorization. Classifying data will help determine the type of security controls appropriate for safeguarding that data. A data classification policy should define PPSI, explain the reasons for collecting this information, define procedures for its access and provide for the use, storage and disposal of this data.

City officials have not developed written policies and procedures for managing PPSI collected, processed, transmitted and stored. Without formal policies and procedures, officials do not have adequate assurance that this data is effectively and adequately protected from unauthorized access. In addition, City officials and employees may not understand what constitutes sensitive information and how to adequately safeguard it. Further, City officials may not be prepared to notify affected persons in a timely manner in case of a security breach.

Cyber Security Training — The IT security community often identifies people as the weakest link in the chain to secure data and systems. Good internal controls should include employee IT security training and awareness efforts that are closely tied to the City's IT policies. City officials cannot protect the confidentiality, integrity and availability of data and computer systems without ensuring that the people who use and manage IT understand organizational IT security policies and procedures and their roles and responsibilities related to security.

City officials have not developed adequate policies and procedures to ensure that City employees receive proper cyber security training to protect IT assets. The lack of formal cyber security training increases the risk of City employees acting in a manner that could compromise the City's IT assets and security.

Breach Notification Policy — New York State Technology Law[4] requires local governments to establish an information breach notification policy. The policy should detail how officials would notify affected parties whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure should be made in the most expedient timeframe possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

[4] The New York State Information Security Breach and Notification Act is comprised of section 208 of the State Technology Law and section 899-aa of General Business Law.

City officials have not adopted a breach notification policy in accordance with the law. In the event that private information is compromised, City officials and employees may not be prepared to properly notify affected parties, placing them at risk of financial and data loss.

Disaster Recovery Plan — A strong system of IT controls includes a disaster recovery plan that describes how an organization will deal with potential disasters. A disaster could be any sudden, unplanned catastrophic event, such as a fire, flood, computer virus, vandalism or inadvertent employee action that compromises the integrity of the data and the IT systems. Planning to prevent loss of computer equipment and data and establishing procedures for recovery in the event of an actual loss is crucial to an organization.

A disaster recovery plan needs to address the roles of key individuals and include precautions to be taken to minimize the effects of a disaster so the entity will be able to maintain or quickly resume day-to-day operations. In addition, disaster recovery planning involves an analysis of continuity needs and threats to business processes and may include a significant focus on disaster prevention. It is important for City officials to develop a disaster recovery plan, distribute the plan to all responsible parties and periodically test and update the plan to address changes in the City's IT security requirements.

City officials have not developed a disaster recovery plan. Consequently in the event of a disaster, City employees do not have guidance to follow to restore data or resume critical operations in a timely manner. The lack of a disaster recovery plan could lead to loss of important financial and confidential data, in addition to serious interruption of City operations.

Hardware Inventory

Good business practices require management to maintain proper records of IT assets and perform a periodic physical inventory. Accurate and complete inventory records help ensure that assets are properly accounted for. A detailed inventory record for each asset should include a description, make, model, serial number, name of the employee to whom the equipment is assigned (if applicable), physical location and relevant purchase information including the acquisition date. Identification tags should be affixed to each item for easy identification. City officials should periodically examine inventoried equipment to determine its condition and ensure it has not been misplaced or stolen. The IT department is responsible for maintaining an inventory of all assets, including computers and computer-related equipment.

City officials did not develop written policies or procedures governing IT inventory and the City's IT inventory records were incomplete and inaccurate. We attempted to locate 137 computers and three servers listed on the City's inventory record.[5] However, IT department officials were unable to locate any of these items. Asset names and asset identifications were inconsistent. For example, the names of computers listed did not match computers assigned to individuals and asset identification numbers did not match asset serial numbers. In addition, the IT department did not maintain or reconcile inventory periodically.

Without an accurate inventory of computer and technology equipment, City officials cannot be assured that assets are accounted for and protected from loss, theft, misuse and obsolescence. Further in the event of loss, officials would be unable to provide their insurance carrier with an accurate list of assets or determine the items that need to be replaced.

Web Filters

Due to the global nature of the Internet, municipalities today find that it is a nearly indispensable resource for conducting legitimate business activities. However, in recent years, even experienced users have been susceptible to significant threats from cybercriminals who exploit the vulnerabilities of systems and software to gain unauthorized access to sensitive data. For example, computers can be infected by malicious software that, unknown to users, installs and captures computer user identification and password information. Hackers can later use this information to access networks, databases and bank accounts resulting in an increased risk of loss. The City's acceptable use policy defines prohibited uses of City systems.

Internet browsing increases the likelihood that users will be exposed to some form of malicious software that may compromise data confidentiality. City officials should ensure there is an adequate web filtering process in place to limit vulnerabilities in its IT systems through Internet browsing and ensure the City's network is used for appropriate purposes.

To evaluate website use, we reviewed web histories on 26 computers.[6] We searched for website categories that appeared to be personal in nature rather than work related. City employees were able to access websites unrelated to City activities, such as personal online brokerage and trading, personal email and social media.

Although the City's acceptable use policy permits personal use, the web filter does not block categories that are frequently used for high risk personal purposes, such as gambling, file download servers and

[5] City officials were unable to provide information on the value of these items.

[6] See Appendix B for information on our methodology.

proxy avoidance.[7] These categories were in violation of the City's acceptable use policy but not blocked by web filters.

When employees have access to websites unrelated to work or for inappropriate purposes through the City's network, productivity is reduced and there is an increased risk that website contents could put City assets or systems and user information at risk for compromise through malicious software infections.

Online Banking

Online banking offers municipalities the ability to review account balances, make transfers between bank accounts, reconcile accounts and closely monitor cash balances. While there are benefits to online banking, municipal officials need to take steps to avoid fraudulent activities and provide reasonable assurance that cash is properly safeguarded. Therefore, City officials have a responsibility to adopt policies and procedures for online banking which include appropriate controls.

It is important for the City's policy to define the online banking activities the City will engage in; the employees who will be granted access to the City's online accounts; and to include provisions to segregate the duties of initiating, approving, transmitting, recording, and reconciling transactions. The policy must also include provisions for monitoring online banking activity, which requires the reconciliation of a monthly report of all online banking activity with the monthly bank statement to verify that all transactions were appropriate and properly approved.

City officials did not adopt an online banking policy and did not develop procedures for online banking activities. In addition, online banking duties were not properly segregated and account accessibility was not properly controlled. Furthermore, access to the City's bank accounts was not monitored. As a result, we found weaknesses in the controls implemented by City officials for online banking activities, leaving City funds at increased risk of loss.

Electronic Transfers — Electronic transfers can disburse significant amounts of money, usually within minutes of being executed. Some banks offer online wire transfer capabilities allowing officials to initiate, authorize and transmit funds electronically without outside assistance from bank staff. To protect City funds from unauthorized and improper electronic transfers, it is essential that officials ensure that electronic transfers are reviewed and authorized in a timely manner. At least two City officials should be involved in each wire

[7] Proxy avoidance is a way Internet users are able to browse websites that may otherwise be blocked by a network administrator.

transaction, one for authorization and one for transmittal. Also, it is essential that wire transfer confirmations are not performed by the same individual who initiates the transfers.

City officials have not adopted a written policy addressing electronic banking transactions or developed specific written procedures for electronic transfers. We identified five employees with the capability to create, approve and release wire transfers. As a result, these employees are able to make automated clearing house[8] transactions without the review or authorization of any other City employee or official. Because these incompatible duties are not adequately segregated, there is an increased risk that City funds may be improperly transferred or a transfer may be improperly recorded and documented.

Monitoring — The City's online bank accounts must be monitored on a regular basis for unauthorized or suspicious activity. The timely identification and reporting of suspicious activity can help protect the City from loss and improve opportunities for recovery of lost assets.

City officials need to improve their monitoring of online bank account activities. For example, one account was not routinely accessed or monitored for nearly six months. As a result, unauthorized or suspicious online banking activities could go undetected or be identified too late to fully recover losses

Security Controls — Local governments are allowed to disburse or transfer funds in their custody by means of electronic or wire transfer. However, because connecting to the internet is a necessary part of the online banking process, City officials must recognize and prepare for potential vulnerabilities. Therefore, it is important to have controls, such as blocking IP addresses[9] from foreign countries, requiring complex access passwords and regularly changing passwords for online banking activities.

In addition, City officials should have callback procedures in the written banking agreement that require the bank to call someone other than the person initiating the transaction to confirm the appropriateness of the transfer. Weak security controls over online banking increase the risk for cyber-fraud and can result in financial losses that may not be recoverable.

[8] The automated clearing house is an electronic network for financial transactions in the United States, which processes large volumes of credit and debit transactions in batches. Credit transfers include direct deposit, payroll and vendor payments.

[9] An IP address is a unique identifier assigned to each computer and other device (e.g., printer, router, mobile device, etc.) used to communicate over a network.

City officials did not establish appropriate security controls and alerts. City officials provided us with a copy of their bank's generic online policy and security features. City officials did not block wire transfer of suspicious origins (outside the United States) and City employees involved in online banking activities did not receive Internet security awareness training. We also found instances where employees shared their online banking passwords and callbacks features were not established. The lack of appropriate security controls could result in employees unintentionally exposing the City's online bank accounts to malicious software, which could endanger City assets.

Recommendations

City officials should:

1. Update the City's acceptable use policy and ensure that all users of the City's IT assets have signed acknowledgement forms on file.

2. Adopt policies and procedures for breach notification and PPSI protection.

3. Ensure all network users receive IT security training.

4. Develop a formal disaster recovery plan to maintain or restore critical operations as quickly as possible in the event of a disaster. The plan should be distributed to all responsible parties, periodically updated and tested as needed.

5. Establish a comprehensive inventory policy that requires updating the inventory records and performing periodic physical inventories.

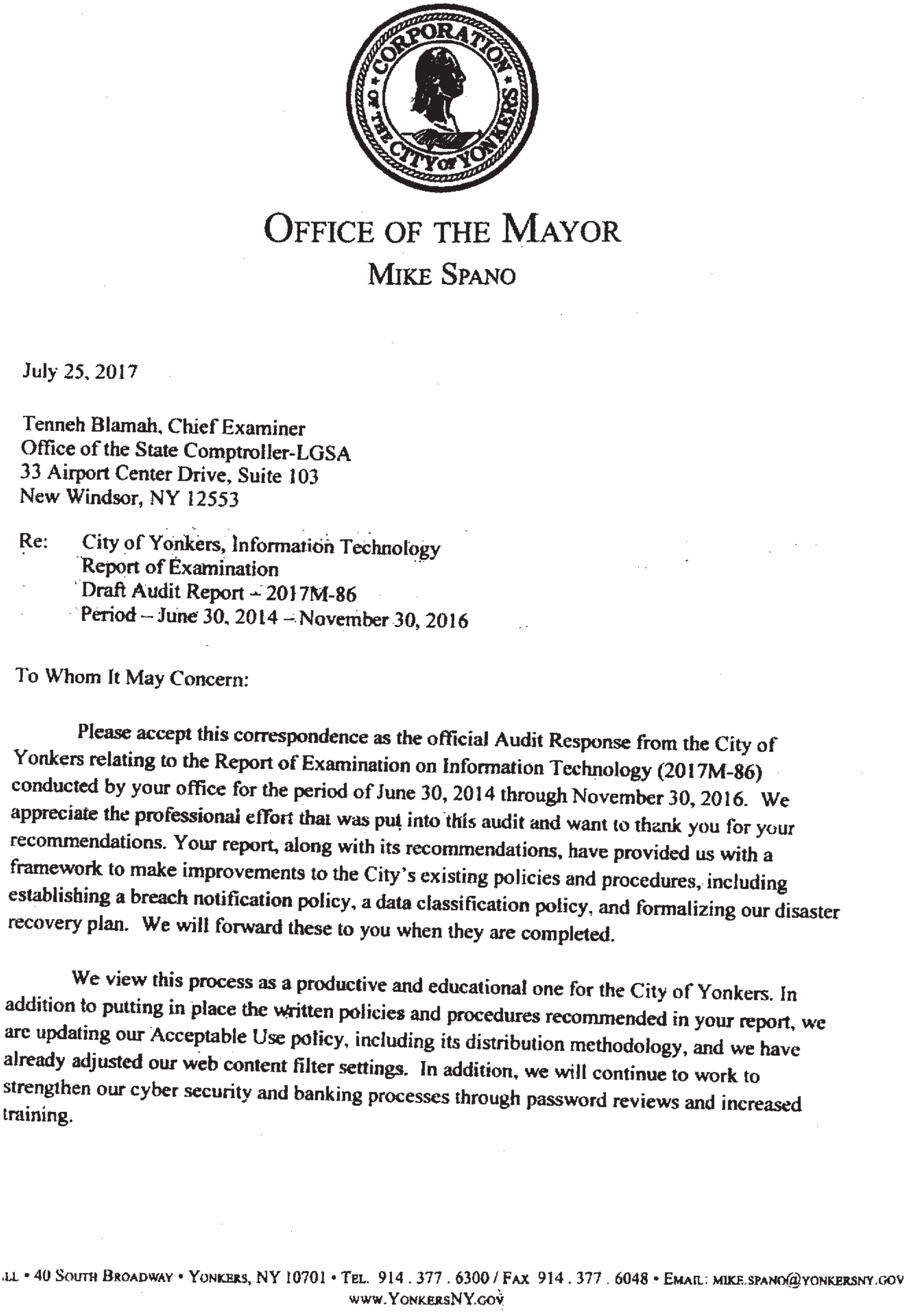
6. Adjust web content filtering to ensure that staff are in compliance with the City's acceptable use policy.

7. Adopt policies and procedures for online banking, segregate incompatible duties of employees, consult with financial institutions and make the necessary changes to increase the security over City funds.

APPENDIX A

RESPONSE FROM CITY OFFICIALS

The City officials' response to this audit can be found on the following pages.



Office of the Mayor

Mike Spano

July 25, 2017

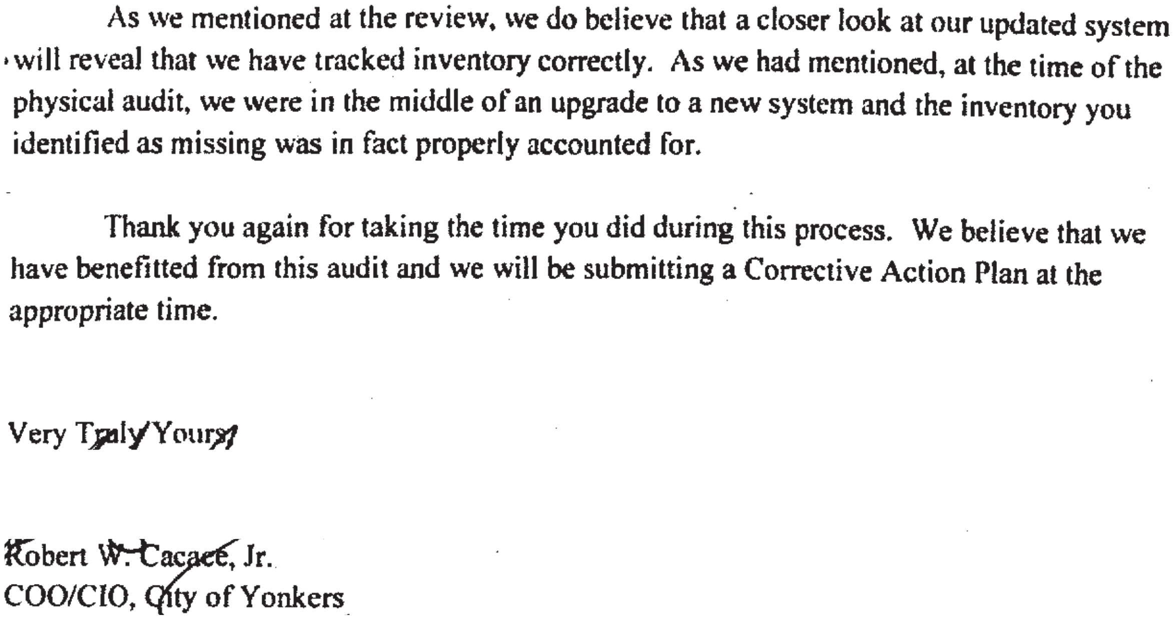
Tenneh Blamah, Chief Examiner
Office of the State Comptroller-LGSA
33 Airport Center Drive, Suite 103
New Windsor, NY 12553

Re: City of Yonkers, Information Technology
Report of Examination
Draft Audit Report – 2017M-86
Period – June 30, 2014 – November 30, 2016

To Whom It May Concern:

Please accept this correspondence as the official Audit Response from the City of Yonkers relating to the Report of Examination on Information Technology (2017M-86) conducted by your office for the period of June 30, 2014 through November 30, 2016. We appreciate the professional effort that was put into this audit and want to thank you for your recommendations. Your report, along with its recommendations, have provided us with a framework to make improvements to the City's existing policies and procedures, including establishing a breach notification policy, a data classification policy, and formalizing our disaster recovery plan. We will forward these to you when they are completed.

We view this process as a productive and educational one for the City of Yonkers. In addition to putting in place the written policies and procedures recommended in your report, we are updating our Acceptable Use policy, including its distribution methodology, and we have already adjusted our web content filter settings. In addition, we will continue to work to strengthen our cyber security and banking processes through password reviews and increased training.



As we mentioned at the review, we do believe that a closer look at our updated system will reveal that we have tracked inventory correctly. As we had mentioned, at the time of the physical audit, we were in the middle of an upgrade to a new system and the inventory you identified as missing was in fact properly accounted for.

See Note 1 Page 17

Thank you again for taking the time you did during this process. We believe that we have benefitted from this audit and we will be submitting a Corrective Action Plan at the appropriate time.

Very Truly Yours,

Robert W. Cacace, Jr.
COO/CIO, City of Yonkers

APPENDIX B

OSC COMMENT ON THE CITY'S RESPONSE

Note 1

Inventory was identified as missing because we were unable to locate, identify or verify the existence of IT equipment. Inventory records were not periodically and routinely updated or reviewed and assets tags and serial numbers were either not reported or improperly recorded.

APPENDIX C

AUDIT METHODOLOGY AND STANDARDS

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

- We reviewed Council minutes for resolutions for IT matters and examined written Council policies to determine the number and scope of policies officially adopted.
- We interviewed City officials and employees to obtain an understanding of City IT operations.
- We reviewed City records for any IT-related policies and procedures.
- We interviewed City employees to determine what safeguards were in place to protect sensitive data and financial assets.
- We reviewed records for 29 employees judgmentally selected based on computer use to determine whether they signed the acceptable use policy acknowledgment form.
- We attempted to locate 137 devices by randomly selecting 14 pages from the City's 134 page inventory record to determine whether they were in the locations listed.
- We judgmentally selected a sample of 30 computers based on assigned users and reviewed Internet browsing histories for personal and high risk activities.
- We obtained reports from the City's web filter to review categories available and the groups of categories available for our previously selected sample.[10] We analyzed the web browsing history for our sample to identify Internet use and pages that disclosed PPSI.
- We reviewed written service-level agreements with the City's IT vendor to determine the scope of services, reporting requirements, performance indicators and security procedures to be provided to the City.
- We interviewed City officials to obtain an understanding of the City's online banking practices.
- We inquired about written agreements with banks and online banking and wire transfer procedures.
- We reviewed accounting records for cost information related to software purchases.

Except for the independence impairment discussed in the Introduction section of this report, 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.

[10] Because of job related duties, we excluded four Police Department computers from our sample for the web browsing history test.

APPENDIX D

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 E

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