DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2017M-184

City of Watertown

Information Technology

DECEMBER 2017

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

Contents

Report Highlights

City of Watertown

Audit Objective

Determine whether City officials adequately safeguarded personal, private and sensitive information (PPSI)[1] on City servers and in its financial system.

Key Findings

- The Council did not adopt policies and City officials did not implement effective procedures for granting, revoking, modifying and monitoring access rights to the City's network and financial system.
- The Council has not adopted adequate information technology (IT) security policies and City officials do not have formal procedures to address disaster recovery, disposal of electronic devices, data back up and password security management.
- The Council did not ensure cybersecurity awareness training was provided to personnel who use City IT resources.

In addition, we confidentially communicated sensitive IT control weaknesses to City officials.

Key Recommendations

- Adopt written IT policies and procedures to address individual access rights, disaster recovery, backups, disposal of electronic devices and password security management.
- Provide IT cybersecurity awareness training to personnel who use City IT resources.

City officials generally agreed with our recommendations and indicated they planned to initiate corrective action.

Background

The City of Watertown (City) is located in Jefferson County. The City is governed by the elected Council composed of four Councilors and a Mayor. The Council is responsible for the general oversight of City operations including adopting policies to safeguard City IT assets. City officials and department heads are responsible for implementing procedures for the policies. The City provides residents with various services including police and fire protection, street maintenance, snow plowing and general government support. To provide these services, the City uses computer servers and other IT assets to store PPSI and share it among various users on the City's network.

Quick Facts	
2016-17 General Fund Budgeted Appropriations	$42 million
Employees	370
Number of City Servers	40

Audit Period

July 1, 2015 – April 5, 2017

[1] PPSI is any information to which unauthorized access, disclosure, modification, destruction or disruption of access or use could severely impact critical functions, employees, customers (residents), third parties or citizens of New York in general.

Information Technology

The City collects and maintains PPSI in various departmental records including tax assessment, birth and death, police reports and payroll. City officials rely on servers, a financial system and other supporting IT equipment to collect, store and manage this information and to share it among various users on the City's network. Access to PPSI on City servers is managed through network user accounts[2] and access to PPSI in the City's financial system is managed through application user accounts.[3] The City's IT Department, composed of the IT Manager and several IT staff members, manages and maintains the network and also adds and removes users from the network and financial system as directed by City officials.

How Should PPSI on the City's Servers and Financial System Be Protected?

Residents and employees rely on City officials to ensure that their personal information on City servers and in the City's financial system is properly safeguarded. City officials are responsible for protecting and preventing improper access to PPSI. To fulfill these responsibilities, the Council should develop and periodically review and update comprehensive written user access policies and City officials should design procedures to protect and monitor access to PPSI. The City should also have IT security policies and procedures for disaster recovery, disposal of electronic devices, backup and password security management to help protect and prevent the loss of important financial data and prevent serious interruption in operations. In addition, to minimize the risk of unauthorized access, management should compare assigned user rights to job duties and periodically review user rights to ensure they are current and appropriate. Management also should verify that terminated users' accounts have been disabled and removed. Lastly, cybersecurity awareness training programs should be provided and directed to users or administrators to reinforce IT policies and focus on security (e.g., the dangers of opening an unknown e-mail or attachment).

The Council Did Not Develop User Access Policies and City Officials Did Not Ensure User Accounts Were Adequately Monitored

The Council did not adopt policies and City officials did not implement effective procedures for granting, revoking, modifying and monitoring individual access rights to the network and the financial system. In addition, City officials need to improve the management of network and financial system user accounts.

[2] A network user account grants access to resources, including servers and computers, within the network on which that user account exists.

[3] An application user account grants access to data in and functionality provided by the application within which that user account exists.

We examined the 612 user accounts that grant access to the City network and found that 192 (31 percent) are no longer necessary. The IT Manager was unsure whether another 55 (9 percent) are necessary. Seventy of these 247 accounts have never been used and another 26 have not been used in at least seven years. The IT Manager told us he sometimes reviews active network user accounts and deletes the active accounts for individuals he is aware left City employment. However, there is no formal policy or procedure for doing so.

In addition, 286 of the 612 (47 percent) network user accounts are generic and/or shared. They may be used by more than one individual. Therefore, officials could have difficulty managing these accounts and removing or disabling those no longer needed because it may not always be clear exactly who uses these accounts and whether the access is needed. Further, without requiring users to enter unique usernames and passwords for these accounts, officials cannot grant access specific to users' job duties and cannot trace suspicious activity to a specific individual.

We also compared the City's payroll reports to the list of all 75 individuals who have access to the City's financial system to determine whether users are currently employed with the City and should have access.[4] Four individuals, who were no longer employed with the City, still had active user accounts to the financial system.[5] We also reviewed the access permission levels for each financial system user and found no material exceptions when compared to the employee's actual job duties.

Without adopted policies and procedures for monitoring and revoking user access rights, City officials did not have an effective process in place to notify IT officials of changes to employees' employment status. This resulted in unnecessary user accounts in the network and financial system. Unnecessary network and financial system user accounts should be disabled or removed as soon as they are no longer needed to decrease the risk of unauthorized access and potential entry points for attackers to copy, manipulate or delete PPSI. Of particular risk are user accounts for former employees, as these could potentially be used by those individuals for malicious activities. Further, unnecessary accounts create additional work to manage access, along with the risk of errors that could result in users being inadvertently granted more access than needed.

[4] See Appendix B for Methodology

[5] At the end of fieldwork, the IT Manager told us that all four user accounts have been disabled.

The Council and City Officials Did Not Adopt Adequate IT Security Policies and Procedures

The Council has not adopted a comprehensive disaster recovery plan to describe how City officials will deal with potential disasters, which could include sudden, unplanned catastrophic events (e.g., fire, computer virus or inadvertent employee action) that compromises the availability or integrity of the network and financial system. Typically, a disaster recovery plan involves the analysis of business processes and continuity needs, a focus on disaster prevention, the roles of key individuals and the precautions to maintain or quickly resume operations.

In addition, there are no adopted policies for the disposal of electronic devices or procedures for the City's contract with an outside vendor for disposal services. Therefore, officials do not have guidelines to confirm that the equipment planned for disposal was actually disposed or that such equipment was free of PPSI.

Also, there are no adopted policies and procedures for data backup that define the frequency and scope of backups, the location of stored back up data, and the specific method for backing up (e.g., encryption). The City does not store its backups of network and financial information in an offsite location. Even though City officials back up data at regular intervals, they should verify that the data has been backed up and can be restored. Lastly, the Council has not adopted adequate policies and procedures for password security management to define how passwords should be controlled to ensure the highest level of security over PPSI.

Without established policies and formal procedures addressing disaster recovery, disposal of equipment, backup of data and password security, there is an increased risk that the City could lose important financial data, improperly dispose of equipment containing PPSI and suffer serious interruption in operations.

Users Have Not Received Cybersecurity Awareness Training

The Council has adopted an acceptable use policy for the use of City-owned computers, e-mail and the Internet. However, users have not received security awareness training to help ensure they understand security measures to protect the City's network. As a result, the City's IT assets and PPSI are more vulnerable to loss and misuse. For example, users may not be prepared to recognize and appropriately handle malicious e-mail messages, which increases the risk of a ransomware or other type of malware infection on City computers.

What Do We Recommend?

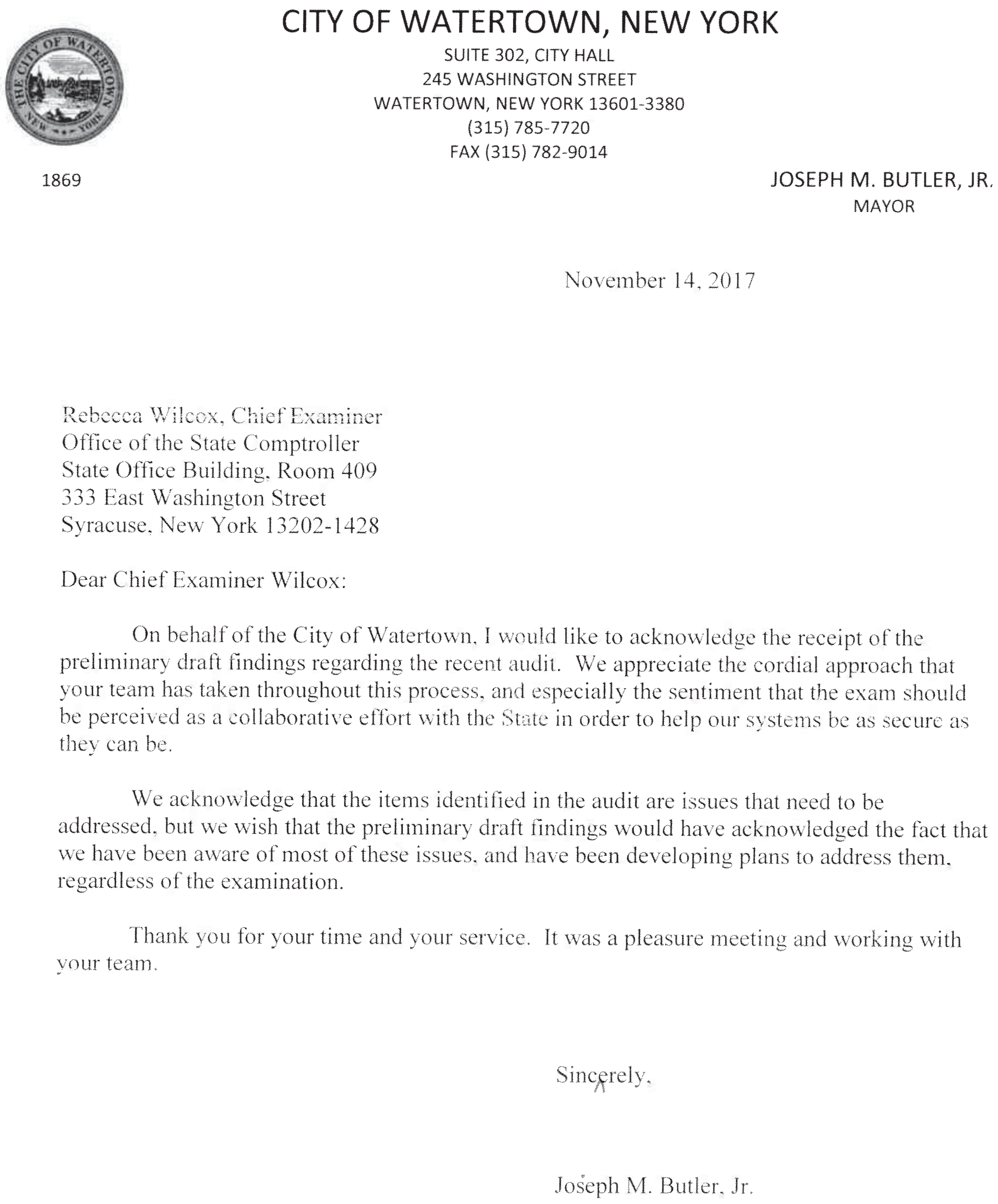
The Council should:

1. Adopt written IT policies to address individual access rights, disaster recovery, backups, disposal of electronic devices and password security management.
2. Periodically review and update all IT policies to reflect changes in technology and the City's computing environment.
3. Ensure IT cybersecurity awareness training is provided to personnel who use City IT resources.

The IT Manager and City officials should:

4. Evaluate all existing network and financial system user accounts, disable or remove any deemed unnecessary and periodically review for necessity and appropriateness.
5. Determine whether the use of shared accounts is appropriate or if network access should be limited to unique user accounts.
6. Ensure procedures are implemented for any IT policies adopted or updated by the Council.

Appendix A: Response From City Officials



CITY OF WATERTOWN, NEW YORK

SUITE 302, CITY HALL
245 WASHINGTON STREET
WATERTOWN, NEW YORK 13601-3380
(315) 785-7720
FAX (315) 782-9014

1869

JOSEPH M. BUTLER, JR.
MAYOR

November 14, 2017

Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
State Office Building, Room 409
333 East Washington Street
Syracuse, New York 13202-1428

Dear Chief Examiner Wilcox:

On behalf of the City of Watertown, I would like to acknowledge the receipt of the preliminary draft findings regarding the recent audit. We appreciate the cordial approach that your team has taken throughout this process, and especially the sentiment that the exam should be perceived as a collaborative effort with the State in order to help our systems be as secure as they can be.

We acknowledge that the items identified in the audit are issues that need to be addressed, but we wish that the preliminary draft findings would have acknowledged the fact that we have been aware of most of these issues, and have been developing plans to address them, regardless of the examination.

Thank you for your time and your service. It was a pleasure meeting and working with your team.

Sincerely,

Joseph M. Butler, Jr.

Appendix B: Audit Methodology and Standards

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law. To achieve the audit objective and obtain valid audit evidence, we performed the following audit procedures:

- We obtained and reviewed City policies and procedures related to IT.
- We inquired with City officials about the process followed, including written guidelines, for granting access to the City's network and financial system, reviewing specific access and permissions granted to individual users, and removing and modifying permissions in a timely manner.
- We provided an audit script to the IT Manager on a universal serial bus (USB) drive to run on the City's domain controllers.[6] We analyzed each report generated by the script, looking for potentially unnecessary user accounts.
- We reviewed a user permission report from the City's financial system to determine the appropriateness of the permissions granted to each user in relation to the users' actual job duties.
- We obtained a list of all users of the City's financial system and compared it to the payrolls to determine whether any users were not employed with the City.
- We interviewed City officials to determine whether employees received cybersecurity awareness training.

Our audit also examined the adequacy of certain information technology controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to City officials.

We conducted this performance audit in accordance with GAGAS, generally accepted government auditing standards. 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.

[6] A domain controller is a server that manages access to resources on a network via user accounts, permissions and security policies.

A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and provided to our office within 90 days, pursuant to Section 35 of 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 the CAP available for public review in the Clerk's office.

Appendix C: Resources and Services

Regional Office Directory

http://www.osc.state.ny.us/localgov/regional_directory.pdf

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management

http://www.osc.state.ny.us/localgov/pubs/listacctg.htm#lgmg

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans

http://www.osc.state.ny.us/localgov/planbudget/

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller

http://www.osc.state.ny.us/localgov/finreporting/

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
http://www.osc.state.ny.us/localgov/costsavings/

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
http://www.osc.state.ny.us/localgov/fiscalmonitoring/

Research Reports / Publications – Reports on major policy issues facing local governments and State policy-makers
http://www.osc.state.ny.us/localgov/researchpubs/

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

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.state.ny.us

www.osc.state.ny.us/localgov

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

SYRACUSE REGIONAL OFFICE – Rebecca Wilcox, Chief Examiner

State Office Building, Room 409, 333 E. Washington Street, Syracuse, New York 13202-1428

Tel: (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

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