DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2019M-22

City of Middletown

Water System Cybersecurity

NOVEMBER 2019

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

City of Middletown

Audit Objective

Determine whether City officials adequately safeguarded electronic access to the City's water system.

Key Findings

- Officials did not have adequate policies and procedures to document employee IT security duties, provide guidance for using portable devices or require monitoring of networked water system devices.
- Officials did not provide employees with IT security awareness training.

In addition, sensitive information technology (IT) control weaknesses were communicated confidentially to officials.

Key Recommendations

- Develop and implement sufficient IT policies and procedures for the water system.
- Provide IT security awareness training to City employees at least annually.

City officials agreed with our recommendations and have initiated or indicated they planned to initiate corrective action.

Background

The City of Middletown (City) is located in Orange County. The City is governed by a Mayor, who is elected every four years, and a nine-member Common Council (Council).

The Council is responsible for providing oversight of City operations. The Mayor is the chief executive officer and is responsible, along with other administrative staff, for the City's day-to-day administration.

The Department of Public Works Commissioner is responsible for overseeing water operations, including the day-to-day operations of the water system.

Quick Facts	
Metered Water Sales	$6.7 million
Water Connections	7,443
Customers	28,400
Potable Water Production - 2017	811.3 million gallons

Audit Period

January 1, 2017 – September 21, 2018. We extended our audit period forward through November 21, 2018 to complete our IT testing.

Water System Cybersecurity

The City maintains a computer-based water system to control and monitor water flows, levels, pressure and quality characteristics (such as pH, temperature and turbidity). Officials contract with a third-party vendor to manage the water systems' information technology (IT) components (e.g., computers and network devices) and with another third-party vendor to manage the day-to-day operations of the water plant.

How Should Water Systems Be Protected?

A disruption to a city's water system could range from a minor inconvenience to serious consequences relating to the health of personnel and water customers. A city's governing board and water plant officials can minimize the risk of disruptions to its water system by adopting and enforcing appropriate IT policies and procedures that document security roles and responsibilities for employees, vendors and consultants and provide guidance for use of mobile storage devices, such as USB flash drives.

Encryption is the process of encoding data so it can be read only by the intended recipient by using a confidential key or password to decrypt the data. Hardware-based encryption is built into a piece of hardware, such as a removable media device, and can be done on a partial- or full-disk basis. A board should develop a mobile storage device policy that requires all mobile storage devices to use an approved method of encryption to protect the data, or use compensating controls such as password-protecting the stored data.

Also, officials should establish procedures for receiving and assessing system cybersecurity alerts and periodically reviewing for Internet-facing devices,[1] which could jeopardize the water system. In addition, officials should require employees to sign acknowledgement forms to indicate they have received water system policies and procedures and to ensure employees are aware of and understand what is expected of them.

The City Did Not Have Adequate Policies and Procedures

Although City officials developed informal procedures related to the security of the water system, they did not have any written policies or procedures. There were no policies and procedures to document security roles and responsibilities for employees, vendors and consultants; explain appropriate use of mobile storage devices, such as USB flash drives[2]; or require monitoring and logging of networked and Internet-facing devices.[3] Because there were no written

[1] Internet-facing devices either have Internet capabilities or can be communicated with from the Internet.

[2] A USB flash drive is a portable data storage device.

[3] The water system consisted of a series of devices that communicated and interacted on a network. Because many of these devices had Internet-access capabilities, they should have been monitored to help ensure they were used as intended, had not been compromised and were currently authorized to connect to the water system.

policies and procedures, officials could not ensure employees were aware of or understood what was expected of them in maintaining the security of the water system.

In October 2017, City officials hired a third-party vendor to conduct an assessment of the City's water system who recommended that officials develop a cybersecurity policy. However, officials did not implement this corrective action. Without adequate policies and procedures, the City had a greater risk that its water system could have been compromised by attackers or that employees could have inadvertently compromised security measures.

Why Should Officials Provide IT Security Awareness Training?

To minimize the risk of unauthorized access to the water system and misuse or loss of data, officials should provide annual IT security awareness training that explains IT security measures and cybersecurity risks specific to industrial control systems (ICS)[4] and communicates related policies and procedures to all water system employees. The training should center on emerging trends such as information theft, social engineering attacks[5] and computer viruses and other types of malicious software. Training programs should be directed at the specific audience and include everything that attendees need to perform their jobs.

The training should also cover key security concepts such as the dangers of downloading files and programs from the Internet, using portable devices such as USB drives, the importance of selecting strong passwords, any requirements related to protecting PPSI,[6] risks involved with using unsecured Wi-Fi connections or how to respond if a virus or an information security breach is detected.

Employees Did Not Receive IT Security Awareness Training

City officials did not provide water system employees with IT security awareness training. The IT cybersecurity community identifies people as the weakest link in the chain to secure data and IT systems. Officials cannot protect the confidentiality, integrity and availability of data and computer systems without ensuring that employees understand their roles and responsibilities related to IT and data security.

[4] An ICS gathers information on an industrial process and modifies, regulates or manages the process to achieve a desired result.

[5] Social engineering attacks are methods used to deceive users into revealing confidential or sensitive information.

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

Without IT security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise IT assets. In addition, because the water system did not have adequate IT policies, employees were not provided with limitations on how they should use IT assets. As a result, the water system had a significant risk that users could inadvertently put the water system and its related data at risk for unauthorized access, misuse or abuse.

What Do We Recommend?

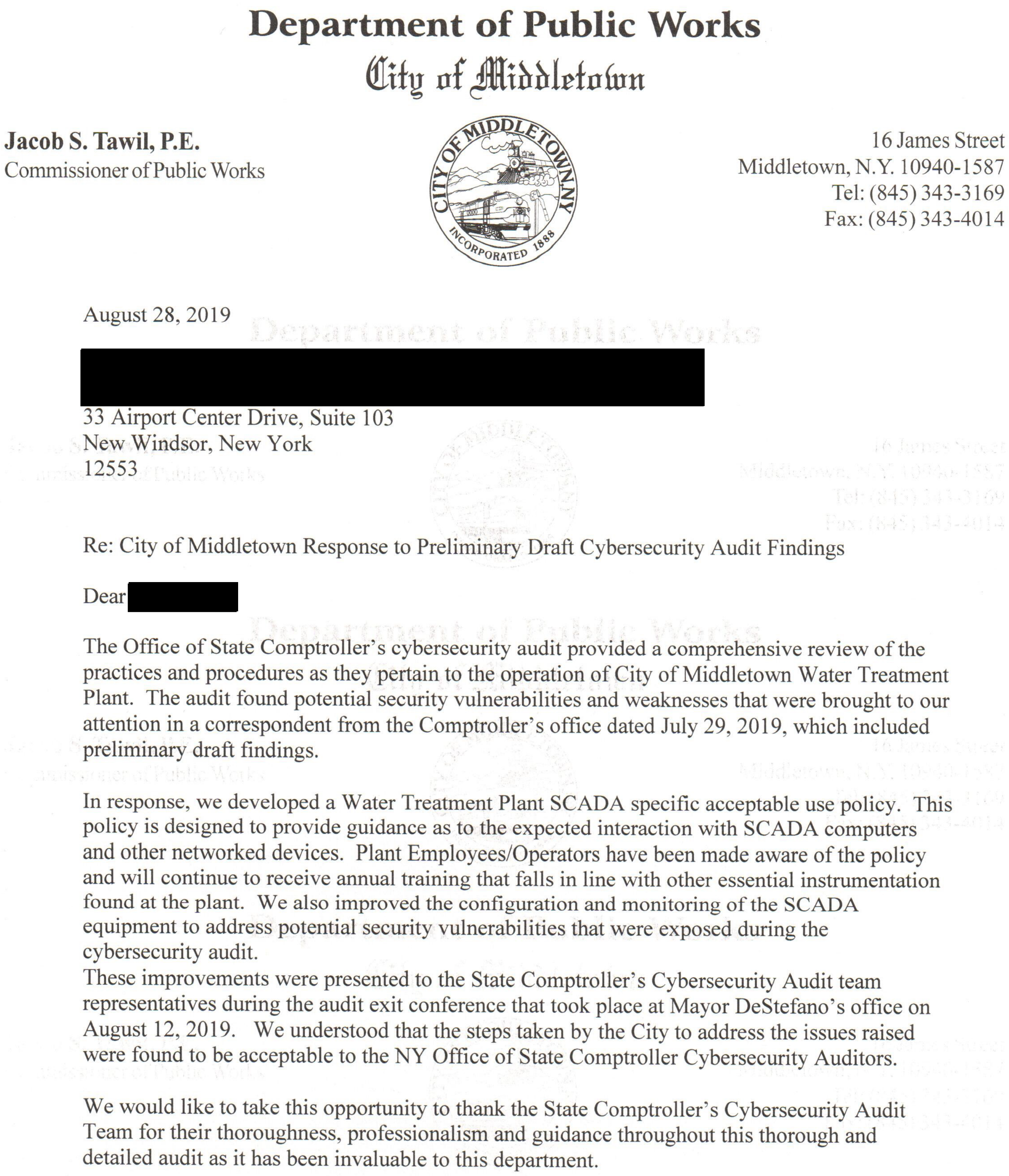
The Council should:

1. Develop and implement policies and procedures that document the roles and responsibilities of employees, contractors and consultants; explain appropriate use of mobile storage devices, such as USB flash drives; and require monitoring and logging of network devices.

2. Consider requiring employees to sign acknowledgement forms to help ensure they are aware of and understand what is expected of them.

3. Ensure that all City employees who have access to the water system receive IT security awareness training at least annually.

Appendix A: Response From City Officials



Department of Public Works

City of Middletown

Jacob S. Tawil, P.E.
Commissioner of Public Works

16 James Street
Middletown, N.Y. 10940-1587
Tel: (845) 343-3169
Fax: (845) 343-4014

August 28, 2019

[redacted]
33 Airport Center Drive, Suite 103
New Windsor, New York
12553

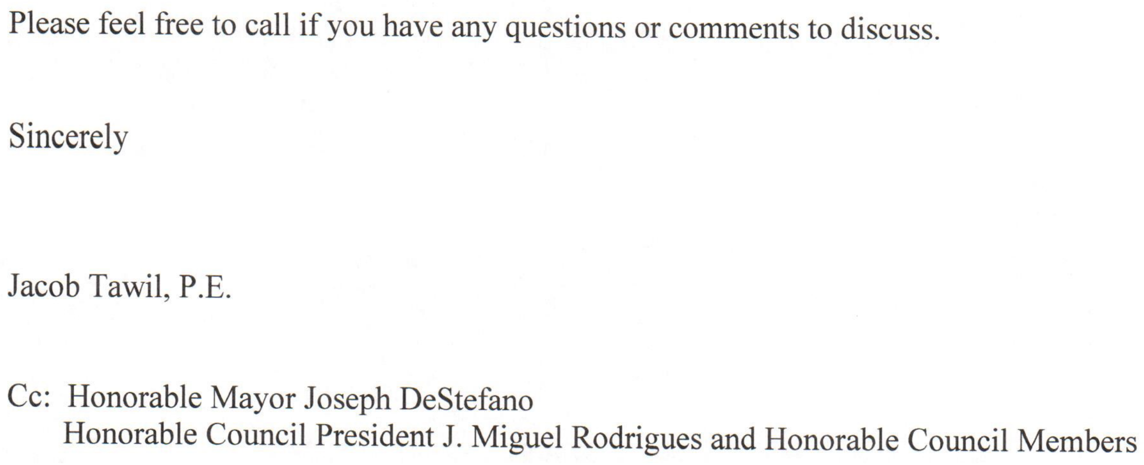
Re: City of Middletown Response to Preliminary Draft Cybersecurity Audit Findings

Dear [redacted]

The Office of State Comptroller's cybersecurity audit provided a comprehensive review of the practices and procedures as they pertain to the operation of City of Middletown Water Treatment Plant. The audit found potential security vulnerabilities and weaknesses that were brought to our attention in a correspondent from the Comptroller's office dated July 29, 2019, which included preliminary draft findings.

In response, we developed a Water Treatment Plant SCADA specific acceptable use policy. This policy is designed to provide guidance as to the expected interaction with SCADA computers and other networked devices. Plant Employees/Operators have been made aware of the policy and will continue to receive annual training that falls in line with other essential instrumentation found at the plant. We also improved the configuration and monitoring of the SCADA equipment to address potential security vulnerabilities that were exposed during the cybersecurity audit.
These improvements were presented to the State Comptroller's Cybersecurity Audit team representatives during the audit exit conference that took place at Mayor DeStefano's office on August 12, 2019. We understood that the steps taken by the City to address the issues raised were found to be acceptable to the NY Office of State Comptroller Cybersecurity Auditors.

We would like to take this opportunity to thank the State Comptroller's Cybersecurity Audit Team for their thoroughness, professionalism and guidance throughout this thorough and detailed audit as it has been invaluable to this department.



Please feel free to call if you have any questions or comments to discuss.

Sincerely

Jacob Tawil, P.E.

Cc: Honorable Mayor Joseph DeStefano
Honorable Council President J. Miguel Rodrigues and Honorable Council Members

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, our audit procedures included the following:

- We interviewed City officials, employees and relevant third-party personnel to gain an understanding of the City's water system and related cybersecurity controls.
- We reviewed written agreements between the City and its contracted water system vendors.
- We inspected the water plant and supporting infrastructure and reviewed documentation filed with the New York State Department of Health.
- We performed a search to identify whether any water system devices that had Internet-access capabilities were identified on the Internet, which could make them susceptible to being compromised.

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 City 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.

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 City clerk's office.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/localgov/regional_directory.pdf

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

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

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/localgov/pubs/listacctg.htm#lgmg

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/localgov/planbudget/index.htm

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/localgov/pubs/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/localgov/finreporting/index.htm

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

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

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/localgov/index.htm

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

NEWBURGH REGIONAL OFFICE – Lisa A. Reynolds, Chief Examiner

33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725

Tel (845) 567-0858 • Fax (845) 567-0080 • Email: Muni-Newburgh@osc.ny.gov

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

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