DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2017M-117

City of Glens Falls

Water and Wastewater System Cybersecurity

NOVEMBER 2017

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

City of Glens Falls

Audit Objective

Determine whether officials adequately safeguard electronic access to the City's water and wastewater systems.

Key Findings

- Officials could better safeguard the City's water and wastewater systems.
- There is no formal process for staying current on system cybersecurity threats.
- Officials have not provided employees with cybersecurity awareness training.
- Officials do not prevent or monitor public disclosure of information that could jeopardize the City's systems.

In addition, sensitive information technology control weaknesses were communicated confidentially to City officials.

Key Recommendations

- Establish a process for receiving and assessing system cybersecurity alerts.
- Provide cybersecurity awareness training to City employees.
- Prohibit the disclosure of information that can jeopardize the City's systems and monitor for and remove such publicly shared information.

City officials generally agreed with our recommendations and plan to initiate corrective action.

Background

The City of Glens Falls (City) is located in Warren County. The elected six-member Common Council (Council) is responsible for managing the City's operations. The Water and Sewer Commission is responsible for overseeing water and wastewater operations. The Water and Sewer Superintendent (Superintendent) is responsible for managing the day-to-day operations of the water and wastewater systems.

Quick Facts

2017 Budgeted Appropriations	
General Fund	$17.8 million
Water Fund	$3.4 million
Sewer Fund	$6.0 million
Employees	210
Residents	14,300
Water Customers	14,600
2016 Daily Averages	
Water Treated	2.3 million gallons
Wastewater Treated	3.5 million gallons

Audit Period

January 1, 2015 - February 28, 2017

Water and Wastewater System Cybersecurity

The City maintains computer-based systems to control and monitor water and wastewater flows, levels, pressure and quality characteristics (such as pH, temperature and turbidity). Officials contract with a third-party vendor to manage the information technology (IT) components (e.g., computers and network devices) of the City's water and wastewater systems and with another third-party vendor to manage the operational technology components (e.g., programmable logic controllers) of the wastewater system. A disruption to a City system could range from a minor inconvenience to serious consequences relating to the health of both employees and water consumers.

How Should Water and Wastewater Systems Be Protected?

The Superintendent and the Council can minimize the risk of disruptions to the City's water and wastewater systems by establishing a process for receiving and assessing system cybersecurity alerts; adopting and enforcing a computer and Internet use policy; providing cybersecurity awareness training to all City employees at least annually; prohibiting vendors from disclosing information about the City's systems and periodically reviewing publicly available content for information that could jeopardize the systems.

The City Does Not Stay Current on Cybersecurity Threats

The Superintendent has not established a formal process for staying current on system cybersecurity threats. Water and wastewater personnel do not receive alerts to such threats from key sources including the U.S. Department of Homeland Security's Industrial Control System Cyber Emergency Response Team (ICS-CERT) or the Water Information Sharing and Analysis Center (WaterISAC). The Superintendent indicated that they rely on the City's third-party vendors for threat information. However, we found no evidence that such information is routinely shared and the service level agreements between the City and these vendors do not require them to do so. Without taking proactive steps to stay current on cybersecurity threats, officials cannot adequately safeguard the City's systems against those threats.

Employees' Internet Use Puts City Systems at Risk

The Council adopted a policy in October 2014 that prohibits personal use of the Internet and City computers during working hours. However, we found that City employees do not adhere to this policy and City officials do not enforce adherence to it. Some employees use the Internet during working hours to engage in questionable activities that put the City's systems at risk. Specifically, we identified evidence of questionable Internet use on four of 13 examined computers (31 percent) connected to the City's water and wastewater network. City employees used these computers to visit social networking, personal email, shopping, travel and entertainment websites.

Because these types of websites are commonly used to spread malicious software (malware),[1] such Internet use unnecessarily exposes the City's systems to malware infections. While none of the four computers have direct access to either system, if one of the computers becomes infected with malware, the infection could potentially spread to the system and thus lead to a disruption or compromise of that system.

Employees Have Not Received Cybersecurity Awareness Training

Despite our offer to provide introductory-level cybersecurity training focused on water and wastewater systems at no cost to the City in August 2015, officials have not provided employees with this or any other cybersecurity awareness training. While the service level agreement for the City's wastewater vendor includes terms for educational services and operator coaching, these terms are limited to the use and operation of products provided. The City's IT vendor does not provide education or training as part of its services to the City. Without cybersecurity awareness training, employees may not have been aware of the risks of their Internet use and may not be adequately prepared to recognize and respond to malware. This could result in malware infections that lead to a disruption or compromise of a City system.

Officials Do Not Sufficiently Prevent or Monitor for Public Disclosure of City System Information

While the Council has adopted a policy prohibiting disclosure of City information on employees' personal social media accounts, they have not adopted a policy that addresses information shared on the City's public website, and the IT and wastewater vendors are not prohibited from disclosing City system information on the Internet or to prospective clients. The service level agreements between the City and those vendors do not contain terms specific to information disclosure. In addition, no one at the City periodically reviews publicly available content for inappropriate disclosure because the Superintendent has not designated anyone as responsible.

[1] Malware refers to software programs that are specifically designed to harm computer systems and electronic data. Malware often causes this harm by deleting files, gathering sensitive information and making systems inoperable. Computer users can inadvertently install malware on their computers in many ways, including opening email attachments, downloading free software from the Internet or merely visiting infected websites.

We performed a limited search for publicly available information about the City's systems and provided the results to City officials. Individuals with malicious intent commonly search the Internet for system details (e.g., discussions of specific operating systems and software, or where and how technology is deployed) while planning their attacks. Exposing such details unnecessarily provides information to these potential attackers, who could then formulate more focused and effective attacks against the City's water or wastewater system.

What Do We Recommend?

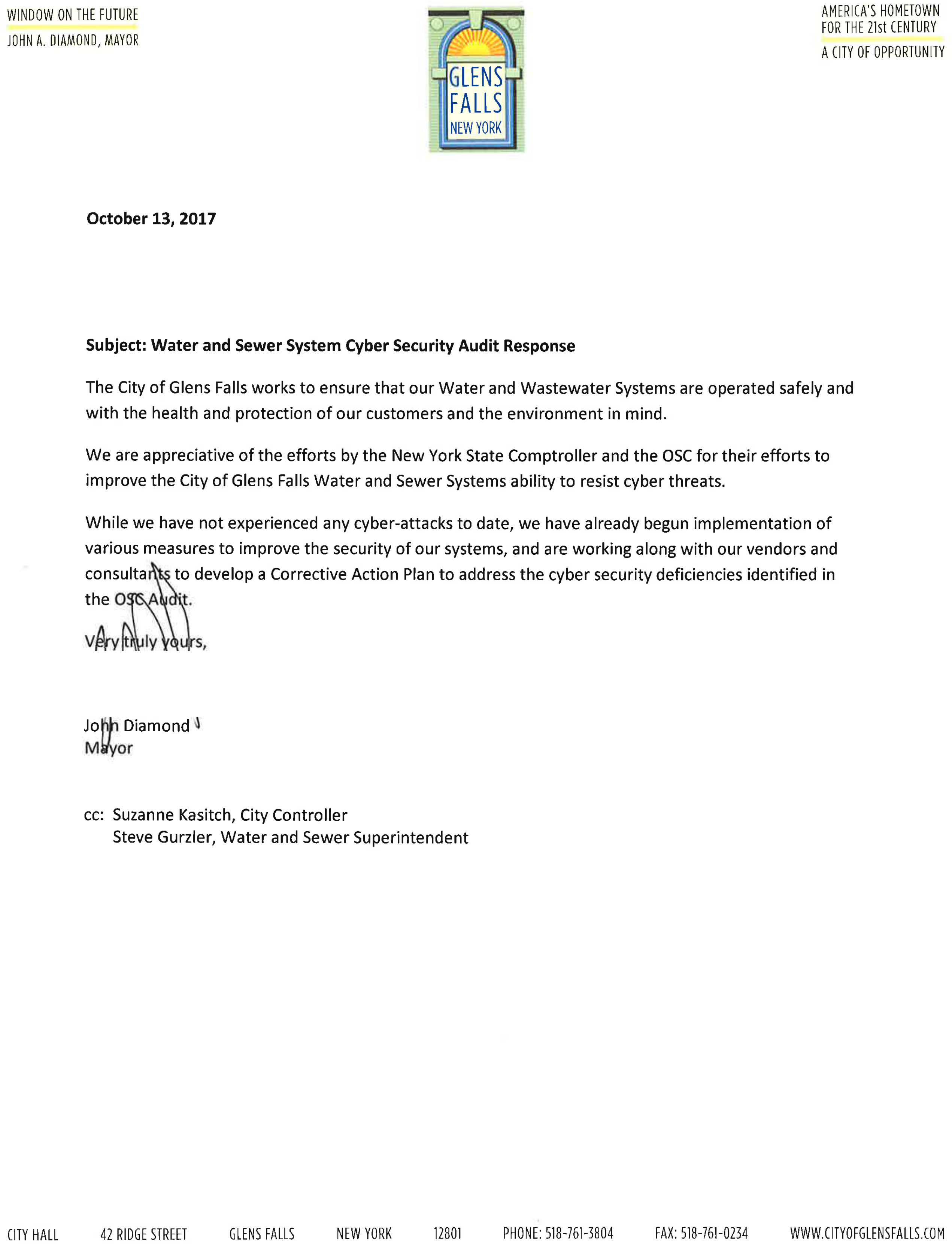
The Superintendent should work with the City's IT and wastewater vendors as needed to:

1. Establish and implement a process for receiving and assessing water and wastewater system cybersecurity alerts.
2. Ensure that City employees are reminded of and adhere to the City's Internet/Computer Use policy.
3. Ensure that all City employees with access to the water and wastewater systems receive cybersecurity awareness training at least annually.
4. Assign someone the responsibility for periodically reviewing publicly available content and ensuring the removal of information that could jeopardize the City's water or wastewater system.

The Council should:

5. Consider including terms in service level agreements to ensure that vendors provide threat information as expected.
6. Adopt a policy that prohibits disclosing information about the City's water and wastewater systems on the City's public website.
7. For future water and wastewater system-related contracts, include terms in service level agreements that prohibit vendors from disclosing information about the City's water and wastewater systems.

Appendix A: Response From City Officials



WINDOW ON THE FUTURE
JOHN A. DIAMOND, MAYOR

GLENS FALLS
NEW YORK

AMERICA'S HOMETOWN
FOR THE 21st CENTURY
A CITY OF OPPORTUNITY

October 13, 2017

Subject: Water and Sewer System Cyber Security Audit Response

The City of Glens Falls works to ensure that our Water and Wastewater Systems are operated safely and with the health and protection of our customers and the environment in mind.

We are appreciative of the efforts by the New York State Comptroller and the OSC for their efforts to improve the City of Glens Falls Water and Sewer Systems ability to resist cyber threats.

While we have not experienced any cyber-attacks to date, we have already begun implementation of various measures to improve the security of our systems, and are working along with our vendors and consultants to develop a Corrective Action Plan to address the cyber security deficiencies identified in the OSC Audit.

Very truly yours,

John Diamond
Mayor

cc: Suzanne Kasitch, City Controller
Steve Gurzler, Water and Sewer Superintendent

CITY HALL 42 RIDGE STREET GLENS FALLS NEW YORK 12801 PHONE: 518-761-3804 FAX: 518-761-0234 WWW.CITYOFGLENSFALLS.COM

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 interviewed City officials, employees and relevant third-party personnel to gain an understanding of the City's water and wastewater systems and related cybersecurity controls.
- We reviewed the written agreements between the City and its IT and wastewater vendors.
- We examined Internet use on 13 computers connected to the City's water and wastewater network.
- We performed Internet searches for publicly available information about the City's water and wastewater systems.

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 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.

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

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

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
http://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
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/index.htm

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
http://www.osc.state.ny.us/localgov/lgli/pdf/cybersecurityguide.pdf

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/index.htm

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

www.osc.state.ny.us/localgov

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

GLENS FALLS REGIONAL OFFICE – Jeffrey P. Leonard, Chief Examiner

One Broad Street Plaza • Glens Falls, New York 12801-4396

Tel (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

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