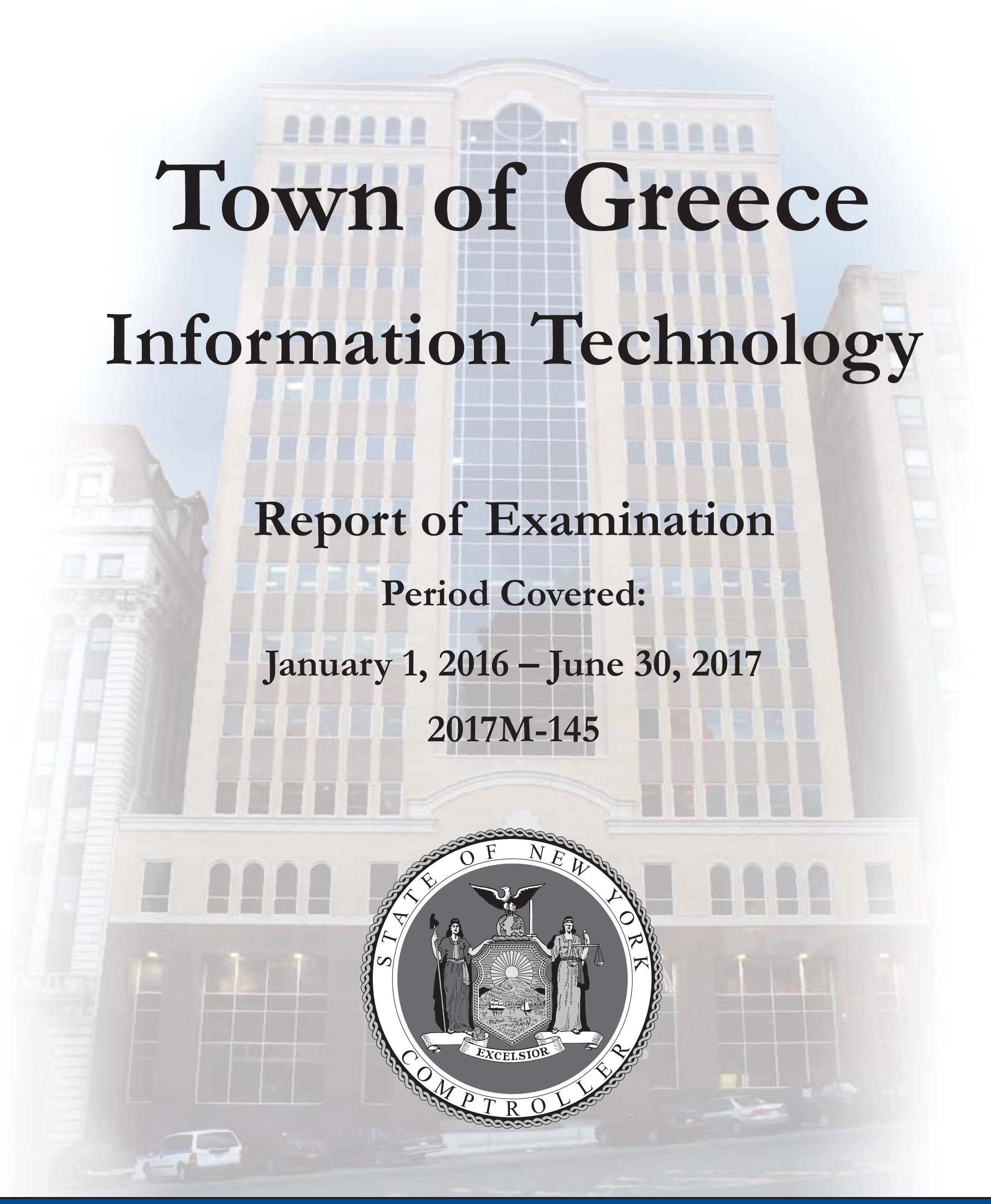
Office of the New York State Comptroller

Division of Local Government
& School Accountability



Town of Greece

Information Technology

Report of Examination

Period Covered:

January 1, 2016 – June 30, 2017

2017M-145

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

January 2018

Dear Town 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 Town Board governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard local government assets.

Following is a report of our audit of the Town of Greece, 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 government 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

EXECUTIVE SUMMARY

The Town of Greece (Town) is located in Monroe County and serves approximately 96,000 residents. The Town is governed by an elected Town Board (Board) comprised of the Town Supervisor (Supervisor) and four Board members, one from each ward. The Board is responsible for the general management and control of Town operations, including financial affairs and security over the information technology (IT) environment. The Town's 2017 appropriations were approximately $56.7 million, which were funded primarily by real property taxes, sales taxes, State aid and fees.

Scope and Objective

We examined the Town's IT controls for the period January 1, 2016 through June 30, 2017. Because our audit examined the adequacy of certain information technology controls, and due to the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to Town officials. The objective of our audit was to evaluate the Town's IT controls. Our audit addressed the following related question:

- Did Town officials adequately safeguard IT assets?

Audit Results

Town officials did not have a comprehensive hardware inventory and can more effectively and efficiently manage software. IT staff did not maintain a comprehensive inventory list of all Town-owned software and purchased software licenses. In addition, the Town's acceptable use policy did not include provisions for enforcement, such as monitoring computer use and reviewing installed software.

Town officials have not developed formal written procedures for regularly reviewing computers. IT staff do not maintain documentation to describe when reviews occurred, what was reviewed and the reviews' results. In addition, Town officials did not have licensing documentation readily available to support the number of licenses purchased. Because certain users have administrative rights that allow them to download and install software without prior permission or approval Town officials must ensure IT staff regularly reviews installed software programs.

Town officials also did not adopt a comprehensive online banking policy or adequately segregate online banking duties. We also found Town officials did not regularly generate or review audit trails[1] or

[1] An audit trail maintains a record of activity by computer system or application that identifies each person who accesses the system, records the time and date of the access, identifies the activity that occurred and records the time and date of log-off.

exception and change reports and did not develop a data classification process. In addition, the Board did not adopt a comprehensive disaster recovery plan. As a result, the Town has an increased risk that its IT data and components may be lost or misused and that the Town will be unable to resume critical operations if a system failure occurs.

Comments of Town Officials

The results of our audit and recommendations have been discussed with Town officials and their comments, which appear in Appendix A, have been considered in preparing this report. Town officials agreed with our findings and indicated they would take corrective action.

Introduction

Background

The Town of Greece (Town) is located in Monroe County and serves approximately 96,000 residents. The Town provides various services to its residents, including highway maintenance, snow removal, lighting, public safety and general government support. The Town's 2017 appropriations were approximately $56.7 million, which were funded primarily by real property taxes, sales taxes, State aid and fees.

The Town is governed by an elected Town Board (Board) comprised of the Town Supervisor (Supervisor) and four Board members, one from each ward. The Board is responsible for the general management and control of Town operations, including financial affairs and security over the information technology (IT) environment. The Supervisor is the chief executive officer and chief financial officer and is responsible for the Town's day-to-day management under the Board's direction. While the Town's IT Director is responsible for its IT environment, the Town also contracts with outside service providers to assist the IT department.

Objective

The objective of our audit was to evaluate the Town's IT controls. Our audit addressed the following related question:

- Did Town officials adequately safeguard IT assets?

Scope and Methodology

We examined the Town's IT controls for the period January 1, 2016 through June 30, 2017. Because our audit examined the adequacy of certain information technology controls, and due to the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to Town 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 Local Officials and Corrective Action

The results of our audit and recommendations have been discussed with Town officials, and their comments, which appear in Appendix A, have been considered in preparing this report. Town officials agreed with our findings and indicated they would take corrective action.

The Board 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 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 Board to make this plan available for public review in the Clerk's office.

Information Technology

IT assets and computerized data are valuable resources that Town officials rely on for making financial decisions, processing transactions, maintaining records and reporting to State and federal agencies. The potential consequences of an IT system failure range from inconvenient to severe. Accordingly, Town officials are responsible for establishing, designing and implementing a comprehensive system of internal controls over the Town's IT system.

Town officials should obtain detailed written agreements with service providers and ensure sufficient controls are in place to secure assets when using online banking. In addition, Town officials should manage hardware and software to safeguard Town assets. It is essential to ensure that software controls are in place so that deletions and adjustments cannot be made without authorization and that there is a process in place to review data entered into and changed in the system. Town officials should develop an adequate disaster recovery plan to prevent the loss of computerized data and to help personnel resume operations in a disaster.

Town officials did not have a comprehensive hardware inventory and can more effectively and efficiently manage software. Town officials did not adopt a comprehensive online banking policy or adequately segregate online banking duties. We also found Town officials did not regularly generate or review audit trails[2] or exception and change reports and did not develop a data classification process. In addition, the Board did not adopt a comprehensive disaster recovery plan. As a result, the Town has an increased risk that its IT data and components may be lost or misused and that the Town will be unable to resume critical operations if a system failure occurs.

Hardware Inventory

Town officials should maintain detailed, up-to-date inventory records for all computer hardware. The information maintained for each piece of computer equipment should include a description of the item, including the make, model and serial number; name of the employee to whom the equipment is assigned, if applicable; physical location of the asset; and relevant purchase or lease information with the acquisition date.

[2] An audit trail maintains a record of activity by computer system or application that identifies each person who accesses the system, records the time and date of the access, identifies the activity that occurred and records the time and date of log-off.

Town officials did not maintain a comprehensive hardware inventory. While Town officials provided a hardware inventory upon our request, all computers were not included, and the inventory did not list specific department locations (when necessary) or a specific person who was assigned to the hardware. Although the hardware inventory includes the Town's naming convention for the hardware, it does not include the serial number or purchase information, such as acquisition dates.

Town officials cannot properly protect computer resources if they do not know what resources they have and where they reside. Without a comprehensive hardware inventory, these valuable assets have an increased risk of loss, theft or misuse.

Software Management

The management of software and licenses is essential to safeguarding Town assets and data. Therefore, Town officials should be aware of the software owned by the Town, how it is used and how best to track user rights to ensure licensing compliance. The effective management of software also includes ensuring that only appropriate business software is installed to reduce the risk of unwanted consequences and unnecessary costs that could result from unauthorized software. This can be done, in part, by regularly reviewing computers to identify installed software and taking action to remove any unauthorized software. Town officials should document this review process and its results to provide transparency.

We found that Town officials can manage the Town's software more effectively and efficiently. IT staff did not maintain a comprehensive inventory list of all Town-owned software and purchased software licenses. In addition, the Town's acceptable use policy did not include provisions for enforcement, such as monitoring computer use and reviewing installed software. As a result, Town officials and IT staff did not regularly monitor or review computers to ensure that all software installed was appropriate and legally obtained. We identified inappropriate software installations and software installations that either did not have an adequate number of licenses or did not have sufficient documentation to provide evidence that the Town purchased licenses for the installations.

<u>Software Inventory</u> – The Town should maintain a complete and comprehensive software inventory that includes all software installed on computers with current versions indicated, the number of copies currently in use and any pertinent licensing information, such as the total number of licenses for each software. With a complete, comprehensive software inventory, IT staff can identify software upgrades and patches needed to be installed to address known vulnerabilities.

The purpose of a software license is to grant an end-user permission to use one or more copies of a software program in accordance with copyright law. When a software package is sold, it is generally accompanied by a license from the manufacturer that authorizes the purchaser to use a certain number of copies of the software. Organizations must obtain licenses commensurate with the number of copies in use. Town officials must regularly review all computers to ensure that all software installed is properly approved and licensed.

Town officials did not maintain a software inventory. Although IT staff can generate a report of installed software, the Town does not have a list of authorized software or the total number of licenses purchased for each software application to compare to the number of installations. Upon our request for licensing documentation, the IT Department reviewed purchasing records and created a list of Town-owned software and the number of purchased licenses. However, IT staff did not identify all installed software on Town computers requiring licenses.

Without a complete comprehensive software inventory, it is unlikely that software patches necessary to address known vulnerabilities will be applied on a timely basis, if at all. Additionally, insufficient records increase the likelihood that the Town may inadvertently violate copyright laws, by having more software installations than licenses for particular applications, and incur penalties.

Software Monitoring – The Board is responsible for adopting policies that explain appropriate and inappropriate use of Town IT resources, including expectations concerning personal use of Town computers. Personal Internet usage should be limited to only incidental use and should not include visiting social networking, email and entertainment sites, potentially for nonbusiness purposes, and performing other Internet research and browsing of a personal nature.

Also, a sufficient policy restricts connecting personally owned devices to Town computers. Internet browsing increases the likelihood of exposure to malicious software that may compromise data confidentiality. Further, proper identification of all network devices can help prevent unauthorized devices and the installation of malicious software. Town officials should ensure that there is an adequate web filtering process and procedures to limit vulnerabilities through web browsing and ensure the Town's network is used only for job-related purposes.

Although the Board adopted acceptable use and breach notification policies,[3] it has not ensured that those policies are enforced. The

[3] Refer to the Data Classification section for further information on data security.

Town's acceptable use policy limits personal Internet use to nonwork time and when it is not disruptive to Town business operations. However, the policy does not define unacceptable personal Internet use. The more personal use that is allowed, regardless of the time it occurs, increases the risk to the Town's computers and network. The policy also states that users cannot make or use illegal copies of copyrighted material on the Town network and that computer access will be revoked for users identified as a security risk or with a history of security problems.

Town officials have not developed formal written procedures for regularly reviewing computers. The IT Director told us that the IT department reviews a limited sample of installed software for license compliance on an annual basis, generally Microsoft programs. However, IT staff do not maintain documentation to describe when reviews occurred, what was reviewed and the reviews' results. In addition, Town officials did not have licensing documentation readily available to support the number of licenses purchased.

Because certain users have administrative rights that allow them to download and install software without prior permission or approval Town officials must ensure IT staff regularly reviews installed software programs. We also found a personally owned device connected to a Town computer, which exposed the IT environment to various risks.[4]

We reviewed the software installed[5] on 250 Town computers[6] to determine whether the installed software was authorized, appropriate and licensed, if required, and found that approximately 2,555 programs were generally appropriate. However, we found 17 inappropriate software installations, including 14 instances of malicious software, one installation from a personal device connected (an exercise tracker), one shopping app and one preinstalled video conferencing application that was not removed. In addition, of the 441 installations that required licensing, Town officials did not have sufficient documentation to provide evidence that it purchased an adequate number of licenses for 22 programs.[7]

Although the Town's acceptable use policy permits limited personal use, allowing employees to access nonbusiness-related websites or programs may interfere with their work responsibilities. Additionally, it leaves the Town vulnerable to risk associated with personal use,

[4] Ibid.

[5] There were approximately 2,570 installed programs on the Town's computers. These included drivers, upgrades and components of larger software programs.

[6] Those listed on the May 2, 2017 installed software report

[7] This included two installations of software that is available for personal use, but is not permitted for government use.

including unknowingly downloading viruses and malware by accessing nonbusiness websites or downloading unauthorized software. This increases the risk that the Town could be exposed to unauthorized access, modification to the IT environment or other harmful, malicious events.

Town officials also cannot ensure that software programs are properly licensed, as required by the Town's acceptable use policy, without maintaining sufficient documentation. Further, the Town may incur fines or penalties for installing software that is not properly licensed or permitted for government use.

Online Banking

Online banking provides a means of direct access to funds held in the Town's accounts. Users can review current account balances and account information, including recent transactions, and transfer moneys between bank accounts and to external accounts. Towns are allowed to disburse or transfer funds in their custody by electronic or wire transfers.

Because transfers of funds and automated clearing house (ACH) payments typically involve significant amounts of money, the Town must control the processing of its online transactions to help prevent unauthorized transactions from occurring. Requiring a second authorization or notification of completed transactions provides an added level of security. Town officials should establish procedures to ensure that staff are securely accessing banking websites to help reduce the risk of unauthorized transfers from both internal and external sources.

The Town does not have a comprehensive online banking policy or an adequate agreement with the bank that it uses to access online banking. Additionally, Town officials did not adequately segregate online banking duties.

Policy – To effectively safeguard cash assets, Town officials should establish policies and procedures to monitor and control online banking transactions. A comprehensive online banking policy clearly describes the online banking activities the Town will engage in, specifies which Town employees have the authority to process transactions and establishes a detailed approval process to verify the accuracy and legitimacy of transfer requests.

Although the Board adopted a resolution authorizing the acceptance of signatures for transfers, wire transfers and ACH transactions, and Town officials designated two computers to be used for online banking transactions, the Board did not adopt a comprehensive online banking policy. Without a formal policy that explicitly conveys practices to safeguard data, officials cannot ensure that employees are aware of their responsibilities.

Bank Agreement – General Municipal Law (GML) allows Towns to disburse or transfer funds in their custody by electronic wire transfers, provided that the governing board has entered into a written agreement. GML requires that this agreement prescribe the manner in which electronic or wire transfers will be accomplished, identify the names and numbers of the bank accounts from which such transfers will be made, identify the individuals authorized to request the transfer of funds and implement a security procedure that includes verifying that a payment order is that of the initiating entity and detecting errors in transmission or content of the payment order.

The Town uses one bank for online transactions, including electronic and external wire transfers and ACH payments. The Town's agreement with the bank is a general services agreement that does not contain provisions for how electronic and wire transfers will be performed, including a security procedure, names and numbers of bank accounts from which transfers can be made or individuals authorized to request transfers. As a result, Town officials did not know whether there were dollar limits on the amount that could be transferred. Without an adequate online banking agreement, Town officials cannot be assured that funds are being adequately safeguarded during online transactions.

Segregation of Duties – To adequately safeguard Town assets, Town officials must properly segregate the duties of employees who are granted access to the Town's online banking application. Requiring a second authorization, or notification for completed transfers and changes to the established transfer limits, provides an added level of security over online transactions. A good detective control would be to require banks to provide emails to Town officials alerting them every time an online transaction occurs.

Town officials also could provide an independent review of bank reconciliations to detect and address unauthorized transfers after they have occurred. In the event that these controls are circumvented, Town officials can purchase computer fraud and funds transfer insurance coverage to help recoup a portion of funds misappropriated through computer fraud.

The Town uses one bank for online banking with seven users who have varying levels of access. Three finance department employees can transfer Town funds, the HR Director and payroll clerk have access to upload files for direct deposit and the Tax Collector and Town Clerk have access to their respective department bank accounts.

The three finance office employees can access all bank accounts that the department oversees, and they can make transfers between Town accounts without the authorization of another Town employee. In addition, the bank does not send any notifications to Town officials for these transfers.

Recipients for wire transfers and ACH transactions must be authorized and set up in advance by two individuals approving the recipient in the system. Once they are authorized recipients, one individual can make the wire transfer or ACH transaction, and the bank calls the Director of Finance (Finance Director) to authorize the transaction. The Finance Director told us he can make a transfer, and be the person who approves it, because he is the person designated to receive the bank's phone calls. The bank does not send notification to any other Town employee for these transactions. We reviewed one month of electronic and wire transfers and ACH transactions and found all 77 transactions made during that month were for appropriate Town purposes.

Additionally, due to the limited number of online transfers that can be made in a month, the Finance Director and senior budget analyst go to the bank to make in-person "transfers" by withdrawing from one account and depositing funds in another. During the month we reviewed, these withdrawals totaled more than $776,000. Although we found that deposits were made into other Town accounts, employees could do this without obtaining secondary authorizations.

The Finance Director told us that he monitors bank activity daily. Two finance department employees are primarily responsible for performing bank reconciliations at the end of each month. One of these employees is an online banking user who makes the majority of the Town's online transfers.

While the Finance Director periodically reviews reconciliations when issues arise, there is no routine independent review of bank reconciliations. The Finance Director told us the Town's independent audit firm reviews completed reconciliations as part of the Town's annual audit. However, without a timely, routine independent review of bank reconciliations, inappropriate transactions could remain undetected longer than necessary.

We recognize that Town officials took an additional step to prevent loss by purchasing computer fraud and funds transfer insurance coverage. Although this may not prevent the Town's initial loss, it will provide some reimbursement from actual losses in accordance with the insurance policy. However, the coverage limit is $250,000, and Town account balances are significantly higher.

Data Accuracy and Accountability

Town officials must ensure that adjustments, deletions or other changes to data are appropriate. At a minimum, a designated official – who is not involved in the collection, disbursement and recording of transactions – should approve each adjustment and adequately document the origination of, justification for and amount of the adjustment and date it was approved. Town officials should review audit trails and exception and change reports to monitor user activity and changes to data to provide a mechanism for individual accountability, reconstructing events and problem monitoring.

The Town uses various software programs to prepare building permits; record receipts in the parks and recreation department and Clerk's office; record Court cases, adjudications and collections; and record Town payroll and financial transactions for all funds. During our review of these programs, we identified control weaknesses that could allow users to make adjustments, alterations and deletions without approval, review or detection. For example, both employees in the personnel department can add new employees and adjust pay rates, and the payroll clerk can correct errors in payroll, without authorization.

We also found that the version of Justice Court software used allows users to change receipt numbers and does not have an audit trail function. Further, the financial software does not have a record of transactions. In addition, Town officials are not routinely generating or reviewing exception and change reports to monitor activity for the payroll software or parks and recreation software, which increases the risk that errors and irregularities could occur and remain undetected.

Without requiring authorizations or subsequent review of changes to data, the Town has an increased risk that its data could be misused and altered without detection.

Data Classification

All information, whether in printed or electronic form, should be classified and labeled in a consistent manner to ensure data confidentiality, integrity and availability. The data classification process assigns a risk level to various types of information, which helps management make appropriate data security decisions. Town officials should conduct a data inventory on all equipment to ensure the data classification process is comprehensive. If a data breach occurs, proper data classification and inventorying allows Town officials to determine the extent of unauthorized access and take appropriate action.

The Town's cybersecurity policy states that all information will be classified and managed based on its confidentiality, integrity and availability characteristics. The policy requires that an information security awareness program be developed and additional training be provided to staff using mobile computing devices to raise their awareness on the additional risks inherent with mobile devices.

The IT Director told us that the Town does not have a data classification scheme and that additional training related to the risks of mobile devices has not been provided to mobile device users. Unless Town officials classify the data they maintain and set appropriate security levels, the Town has an increased risk that data could be exposed to unauthorized users and efforts to properly notify affected parties of a data breach will be hampered.

Disaster Recovery Plan

A disaster recovery plan provides a framework for reconstructing vital operations to resume time-sensitive operations and services in a disaster. Such disasters may include any sudden, catastrophic event (e.g., fire, computer virus, power outage or a deliberate or inadvertent employee action) that compromises the availability or integrity of the IT system and data. The plan should describe precautions to minimize the effects of a disaster and enable the Town to maintain or quickly resume critical functions. It also should include a significant focus on disaster prevention and should be distributed to all responsible parties, periodically tested and updated as needed.

The Board entered into an agreement with a security vendor for disaster recovery services, which includes using an off-site location. However, the Board did not adopt a comprehensive disaster recovery plan to address potential disasters.

The IT Director provided us with limited disaster recovery procedures that were insufficient. For example, the procedures consisted of a flow chart for staff to follow that included a box labeled “decide which users will have access.” However, this information should be previously determined and clearly stated within the procedures. Also, the flow chart had another box labeled “give users instructions,” which is vague. The IT Director provided us with instructions for accessing virtual machines,[8] but users will need further instructions. This information should be included in the plan so there is guidance in place if a disaster occurs.

The Town experienced a storm in March 2017 during which staff were able to use the Town building and its equipment. However, Town officials and employees do not have adequate guidance for what to do during a disaster that prohibits the use of the Town hall building and equipment. As a result, the Town risks losing important

[8] A virtual machine is an emulation of a computer system that can be used to remotely access a computer system.

data and disruption of time-sensitive operations, such as processing vendor and payroll checks.

Recommendations

The Board should:

1. Enforce the acceptable use policy, consider amending the policy to define unacceptable personal Internet use and ensure that officials and employees receive adequate Internet security awareness training and training on the Town's IT policies.

2. Adopt a comprehensive online banking policy.

3. Ensure that the Town has a sufficient written online banking agreement.

4. Ensure that officials and employees use the Town's bank notifications and other available security measures for online banking and in-person account transfers, including email notifications that advise Town officials every time an online transaction occurs.

5. Ensure that someone who does not have the ability to make transfers performs timely bank reconciliations.

6. Adopt policies that require authorizations to make adjustments, deletions or other changes to data within the Town's software applications.

7. Adopt a comprehensive disaster recovery plan and ensure the plan is distributed to all essential personnel.

Town officials should:

8. Maintain complete and comprehensive hardware and software inventories.

9. Formalize written procedures to perform regular reviews of software installed on Town computers, ensure that staff properly documents the reviews and compare results to the software inventory list.

10. Ensure that staff maintains adequate software licensing documentation to support the number of licenses purchased.

11. Inquire with the Justice Court software vendor regarding locked receipts and an audit trail and the financial software

vendor regarding a record of activity and periodically generate and review audit trails, exception reports and change reports.

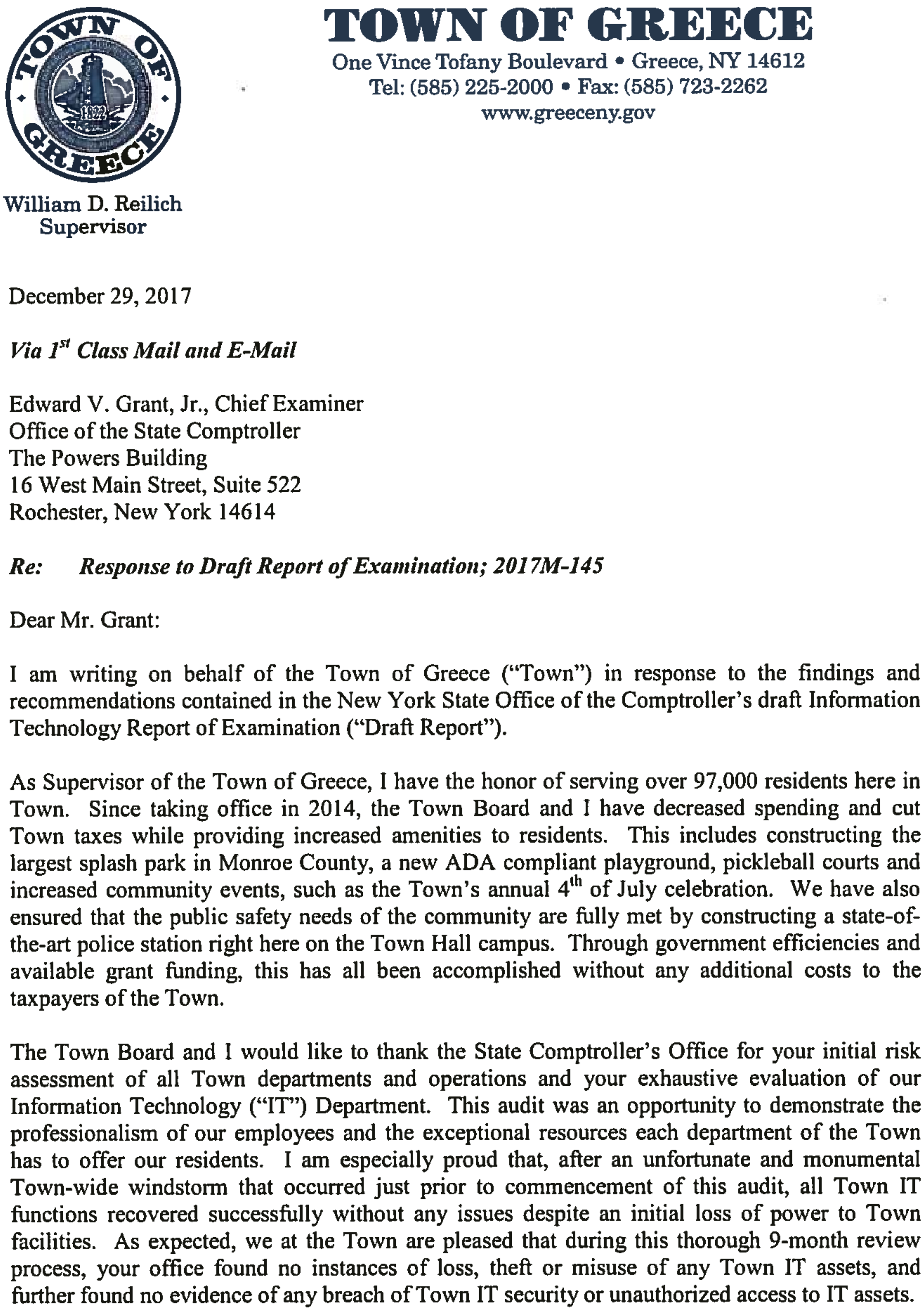
12. Ensure staff prepares a complete classification of data stored on all Town computer equipment and ensure the data classification is updated on an ongoing basis, as appropriate, to reflect any changes.

13. Develop an information security awareness program and provide training to all users, with additional training provided to users of mobile devices to raise their awareness of the additional risks inherent when using the devices.

APPENDIX A

RESPONSE FROM LOCAL OFFICIALS

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



TOWN OF GREECE

One Vince Tofany Boulevard • Greece, NY 14612
Tel: (585) 225-2000 • Fax: (585) 723-2262
www.greeceny.gov

William D. Reilich
Supervisor

December 29, 2017

Via 1st Class Mail and E-Mail

Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street, Suite 522
Rochester, New York 14614

Re: Response to Draft Report of Examination; 2017M-145

Dear Mr. Grant:

I am writing on behalf of the Town of Greece ("Town") in response to the findings and recommendations contained in the New York State Office of the Comptroller's draft Information Technology Report of Examination ("Draft Report").

As Supervisor of the Town of Greece, I have the honor of serving over 97,000 residents here in Town. Since taking office in 2014, the Town Board and I have decreased spending and cut Town taxes while providing increased amenities to residents. This includes constructing the largest splash park in Monroe County, a new ADA compliant playground, pickleball courts and increased community events, such as the Town's annual 4th of July celebration. We have also ensured that the public safety needs of the community are fully met by constructing a state-of-the-art police station right here on the Town Hall campus. Through government efficiencies and available grant funding, this has all been accomplished without any additional costs to the taxpayers of the Town.

The Town Board and I would like to thank the State Comptroller's Office for your initial risk assessment of all Town departments and operations and your exhaustive evaluation of our Information Technology ("IT") Department. This audit was an opportunity to demonstrate the professionalism of our employees and the exceptional resources each department of the Town has to offer our residents. I am especially proud that, after an unfortunate and monumental Town-wide windstorm that occurred just prior to commencement of this audit, all Town IT functions recovered successfully without any issues despite an initial loss of power to Town facilities. As expected, we at the Town are pleased that during this thorough 9-month review process, your office found no instances of loss, theft or misuse of any Town IT assets, and further found no evidence of any breach of Town IT security or unauthorized access to IT assets.

The provided Draft Report includes several recommendations for best practices to be considered by the Town Board and administration relating to IT policies, procedures and inventories. Here at the Town, we are constantly looking to improve operations wherever possible to be as efficient and effective as possible for our residents. This is why I am pleased to report that, as of the date of this letter, the Town has successfully addressed and implemented each recommendation included in the Draft Report. As previously discussed, a comprehensive report will be provided to your office detailing the corrective actions taken to address each recommendation contained in the Draft Report.

The Town Board and I would like to once again thank you for the thorough evaluation and recommendations to assist us in improving our IT-related policies and procedures. We were pleased to learn that this audit and the recommendations will serve as a model to other municipalities throughout the state, and we look forward to continuing to provide residents of this Town with the high level of service they have come to expect.

Very truly yours,

William D. Reilich
Supervisor
Town of Greece

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

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

- We interviewed Town officials and employees to determine the controls and processes in place and gain an understanding of the IT environment.

- We reviewed Board minutes, Town policies, procedures, written agreements, insurance policies and hardware and software inventories.

- We reviewed the report of installed software for May 2, 2017 to identify inappropriate software. We reviewed licensing documentation, including purchase orders, to determine whether the Town maintained the appropriate number of licenses for software installed on Town computers.

- We reviewed all online banking transactions for August 2016 to determine whether they were appropriate Town expenditures. We randomly selected this month from the beginning of our scope period through the month prior to audit notification.

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