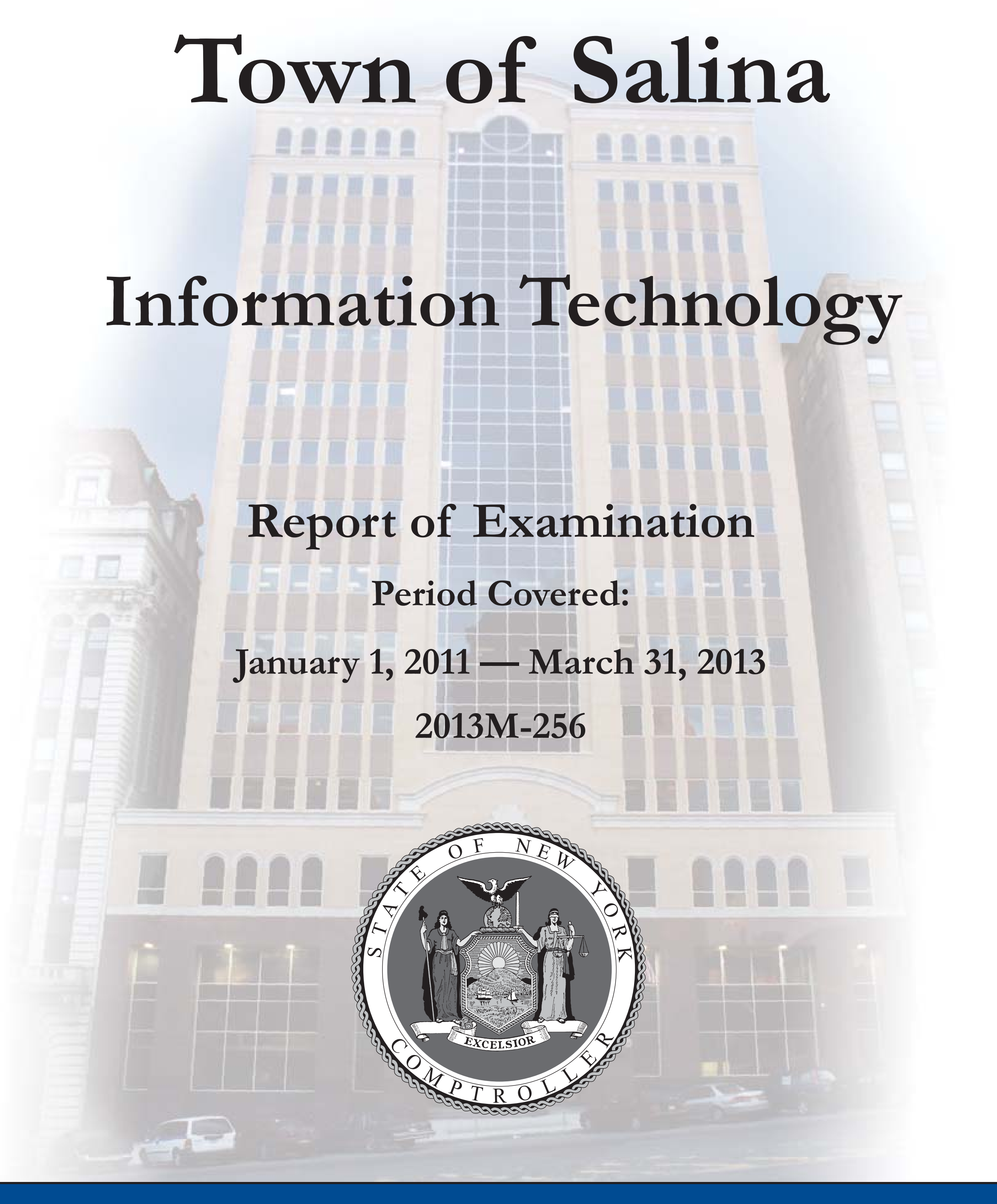
OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY



Town of Salina

Information Technology

Report of Examination

Period Covered:

January 1, 2011 — March 31, 2013

2013M-256

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

November 2013

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 Salina, 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 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

Introduction

Background

The Town of Salina (Town) is located in Onondaga County and has a population of 33,710. The Town is governed by an elected five-member Town Board (Board) which comprises the Town Supervisor and four Board members. The Board is responsible for the general management and control of the Town's assets, including computerized data. The Town Supervisor serves as chief executive officer. The Board appointed a Town Comptroller (Comptroller) who is responsible for the Town's accounting functions. The Town contracts[1] for information technology (IT) services.

The Town's budgeted operating expenditures for the 2013 fiscal year were approximately $14 million, funded primarily with real property taxes and State aid.

Objective

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

- Are internal controls over IT appropriately designed and operating effectively to ensure that the Town's computer equipment and electronic data are adequately safeguarded?

Scope and Methodology

We examined the Town's internal controls over IT for the period January 1, 2011, to March 31, 2013. We extended our audit back to March 2010 to review inventory and July 2008 to review computer disposal records. Our audit disclosed additional areas in need of improvement concerning IT controls. Because of the sensitivity of some of this information, certain vulnerabilities are not discussed in this report, but have been communicated confidentially to Town officials in a separate letter so that they could take corrective action.

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 is included in Appendix B of this report.

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 generally agreed with our recommendations and indicated they planned to take corrective action.

[1] The Town changed contracted IT consultants as of January 1, 2013.

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

Information Technology

The Town's IT system is a valuable and essential part of its operations. It is used for accessing the Internet, communicating by email, processing and storing data, maintaining financial records and reporting to State and Federal agencies. Therefore, it is imperative that Town officials ensure that computerized data is properly safeguarded. Securing technology equipment and electronic storage devices can prevent security breaches that can result in loss of individuals' personal, private and sensitive information (PPSI). Such breaches can be very costly in financial terms and can result in lost productivity, lost confidence on the part of residents and negative publicity. The Board is responsible for establishing policies and procedures to protect the Town's computer equipment and data against the risk of loss, misuse or improper disclosure of sensitive data. This includes developing a comprehensive IT disaster recovery plan to provide guidance on the recovery of data in the event of a disaster.

The Board has not established policies and procedures related to PPSI and sanitizing computer equipment onsite before disposal. In addition, the Board has not instituted policies and procedures to protect data resources. Town officials do not maintain a complete and accurate computer inventory and have not developed an IT disaster recovery plan. Because of these weaknesses, IT assets are at risk for unauthorized, inappropriate or wasteful use. Additionally, in the event of an IT disaster or breach, there is no formal plan of what action Town officials should take to restore service or notify those whose personal information has been compromised.

Personal, Private and Sensitive Information

PPSI is any information to which unauthorized access, disclosure, modification, destruction or disruption of access or use could severely impact critical functions, employees, customers, third parties or citizens of New York. Private information includes one or more of the following: social security number; date of birth; driver's license number or non-driver ID; account number, credit card or debit card number and security code; or access code/password that permits access to an individual's financial (bank) accounts. A good system of IT internal controls starts with policies and procedures to define appropriate user behavior and the tools and procedures necessary to protect PPSI. The policy should have procedures that require the removal of sensitive data and software from computers when they are retired from use, and the responsibility should be clearly assigned.

To be effective in protecting privacy, such a policy should also require that Town officials classify information in a consistent manner to determine the level of security each type of data needs and conduct an inventory of PPSI stored on all their electronic equipment to account for the confidential data they maintain. Town officials should also have written procedures that outline the proper process to use to verify that PPSI is entirely destroyed or removed from electronic equipment prior to the equipment's disposal or reuse.

The Board has not adopted written policies related to the retention and safeguarding of PPSI and does not have a written data classification scheme. There is no policy to address the necessary procedures for the removal of sensitive data from computers and other electronic equipment scheduled for disposal. When Town officials determine that computer and other electronic equipment are no longer needed, they usually move the equipment to a storage room in the Town municipal building. When the room fills up, a maintenance department worker takes the equipment to a third-party vendor hired to recycle the equipment (recycler) for disposal. Town officials do not sanitize the computer hard drives prior to disposal; instead, they rely on the recycler to do the sanitizing. The recycler resells disposed devices and sends unsalvageable devices to the scrap yard. The Town does not have an agreement with the recycler that defines the level of service the recycler will provide and addresses the data protection expectations of the Town. A representative of the recycler told us that Town officials must request sanitization of the computer hard drives at the time they are dropped off or they are sold "as is."

We found an external hard drive that was awaiting disposal in the equipment storage room and determined that it included PPSI and records related to Town employees, such as social security numbers, dates of birth, license numbers, addresses and personnel matters related to suspensions and termination of employment. Town officials cannot be sure that the hard drive would have been wiped clean at the Town's next disposal process, as the Town does not sanitize IT equipment prior to turning it over to the recycler, and the recycler does not sanitize external hard drives unless requested.

In addition, there is no reconciliation between what is removed from inventory and what is actually disposed of through the recycler. The maintenance department worker prepares a disposal list when he takes the items to the recycler; however, the Deputy Comptroller said that she just takes the disposal list and puts it in a folder after the equipment is taken to the recycler. Also, the disposal records do not contain enough information to properly identify the exact computers that are being disposed and some items were listed in the disposal records more than once. Because of these weaknesses, there is an increased risk that the equipment can be disposed of in an improper manner, or misappropriated, which could result in unauthorized users gaining access to confidential and/or sensitive data.

We reviewed inventory and disposal records[2] of the Town's computers and electronic equipment, including copiers, to determine whether the assets were sanitized of sensitive data prior to disposal or transfer. A total of 152 items were disposed of through the recycler, while 32 computers were not disposed of properly through the recycler. Town officials did not follow up to ensure that a copier was sanitized upon return to the manufacturer, as discussed below.

- We identified 19 computers that were no longer in the Town's municipal building. Town officials provided documentation that the recycler sanitized 18 hard drives; however, they were unable to account for the disposal of one computer.

- The Town disposed of a total of 31 computers on July 17, 2008, and October 9, 2009; however, Town officials could not supply documentation of sanitization for any of these computers.

- Town officials returned a copier with a hard drive to the manufacturer at the end of the lease. They signed an agreement to have the leaseholder wipe the hard-drive clean, but Town officials did not have documentation that the machine had actually been wiped clean. The Town did subsequently obtain the documentation during our audit.

As a result of these weaknesses, Town officials do not know the extent to which PPSI resides in the electronic equipment. Further, Town officials cannot be assured the computers and external hard drives designated for disposal have been, or will be, properly disposed of. Unless Town officials classify the data they maintain, set appropriate security levels for PPSI and establish procedures to ensure equipment is properly sanitized prior to disposal, there is an increased risk that PPSI could be inadvertently exposed to unauthorized users when equipment is disposed of.

Breach Notification Policy − State Technology Law requires local governments to establish an information breach notification policy. The policy must detail how employees would notify individuals whose PPSI was, or is reasonably believed to have been, acquired by a person without valid authorization. It is important for the disclosure to be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any

[2] July 17, 2008, 47 items on list; October 9, 2009, 33 items on list; March 8, 2012, 54 items on the list for a total of 134 items disposed of via the recycler

measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. In addition to establishing a breach notification policy, municipalities should notify and train employees of the policy requirements and regularly audit compliance with the policy.

The Town has a breach notification policy[3] in place. The policy appoints the Director of Planning and Development (Director) as "Citizens Notification Officer." However, the Director told us that he was not really familiar with the duties required of the policy because he has not read it in some time.

A breach notification policy is an important tool that provides guidance for staff to follow during a breach event. Employees' lack of knowledge about the adopted policy could seriously jeopardize the effectiveness of the actions the Town takes to protect the public from persons who have obtained personal information without proper authorization.

Inventory Records

Good financial practices require that management maintain proper records of their equipment and perform a periodic physical inventory. Accurate, complete inventory lists help to ensure that inventories are accounted for properly. A detailed inventory record should include a description of the item, including make, model and serial number; the name of the employee to whom the equipment is assigned, if applicable; the physical location of the asset; and relevant purchase or lease information including acquisition date. The items should be periodically examined to establish their condition and ensure they have not been stolen or misappropriated.

We reviewed copies of the Town's technology equipment inventories maintained by the IT consultant.[4] We compared the 2010 inventory list to the 2012 list, which was the most recent inventory list available, and followed up on 47 items taken off the 2012 list to identify equipment that was disposed of. The Town's inventory records were incomplete and inaccurate. Nine computers that had been removed from the inventory list were still in use or stored in various departments rather than the storage room. The Town also had an additional 12 printers on hand that it never added to the inventory lists. For example:

- Both the 2010 and 2012 inventories for the Town courts show one laptop computer. We determined that the two court Justices were using three laptops and we located two

[3] Adopted March 27, 2006

[4] The inventory lists of computers did not include make or model number, but did have the serial number for 57 of 61 computers for 2010 and 56 of 57 for 2012. Printers on the inventory showed make and model, but no serial number.

additional laptops in one Justice's storage room. Due to the lack of identifying make, model or serial number in the inventory records, officials were not able to identify which laptop out of the five was listed on the inventory.

- The Department of Planning and Development purchased five tablet computers in December 2010. The tablet computers replaced five laptop computers on the 2012 inventory list. All five laptop computers are still in the building; however, they are no longer on the inventory list. The Clerk received one laptop computer (it is stored in her vault), one was in the storage room for disposal and three were still in the Planning office.[5]

- The Town's inventory lists 29 printers.[6] We determined that the Town has 41 printers. We traced 10 of the 12 additional printers to the courts, another to the parks and recreation department and the remaining printer to the highway department.

Due to the lack of proper guidance on maintaining inventory lists, lack of facilitation of consistent and accurate recording of technology equipment and lack of periodic reconciliation of lists to ensure items are available at the Town, Town officials cannot be assured that the Town's equipment is adequately accounted for and safeguarded from loss and misappropriation. Therefore, PPSI could be put at risk.

Physical Access to Servers

Physical security over computerized assets is an important component of overall computer and data security. Limiting physical access to the servers to authorized personnel only is necessary to secure the Town's computerized assets and data.

The Town's domain controller was located in the Comptroller's office. The room had two doors: one to the hallway, which was always locked, and one to the office, which was kept open as the room also served as a records storage room. The server was not stored in a locked rack. We found an unlocked door and open network access port in the conference room located on the mezzanine level of the building. This port allowed a direct connection to the Town's internal network and had an unconnected Ethernet cable plugged into it. It is considered best practice to physically secure open rooms by locking the door and disabling open ports. This reduces the likelihood that

[5] Two laptop computers are still being used by the employees they were originally assigned to and one was no longer operational.

[6] No identifying serial numbers are on the inventory list; only the make and model numbers are on the inventory list.

unauthorized users can physically connect to the network and gain access to the Town's data.

Physical threats, whether internal or external, malicious or inadvertent, could lead to damaging or stolen information and/or the release of personal or other confidential information. These security breaches can result in monetary loss and countless staff hours to correct.

Disaster Recovery Plan

IT systems are vulnerable to disruptions from a variety of sources. Examples include natural disasters such as floods and storms, power failures or outages, fire and water damage, vandalism or theft, computer viruses and unintentional user actions. The Town should have a disaster recovery plan, also called a business continuity plan, describing the procedures for data recovery and precautions to minimize the effects of a disaster, so that critical functions can be maintained or quickly resumed. The plan should be distributed to key personnel, periodically tested and updated as necessary to reflect system changes.

The Town does not have a written disaster recovery plan that covers its IT system. Establishing a detailed disaster recovery plan and communicating the plan to key personnel helps ensure they are aware of their responsibilities in preventing, mitigating and responding to emergency situations. Periodically testing the plan, for example, by determining if data that has been backed up can be successfully restored, helps ensure that, in the event of an emergency, the plan will operate as designed. Town officials told us they would rely on their IT consulting firm to help them in the event of an IT disaster and, to continue operation, they would ask another town that uses the same financial system software to share it.

In the event of a disaster causing computer failure, Town personnel have no established guidelines or plan to follow to prevent the loss of equipment and data or to recover data that has been lost or damaged. As a result, this could lead to the loss of financial or operational data, along with a serious interruption of Town operations.

Recommendations

1. Town officials should adopt formal written policies and procedures to ensure a sound IT environment and to protect PPSI.

2. Town officials should complete a classification and inventory of information that the Town maintains to assign the appropriate security level to each type of data and then conduct an inventory of PPSI stored on all their electronic equipment to account for the confidential data maintained. Town officials should update the classification and inventory list on an ongoing basis, as appropriate, to reflect any changes.

3. The Board should establish written policies and procedures to ensure removal of all PPSI data from computers and other electronic equipment prior to reuse or disposal.

4. Town officials should establish a written agreement with the recycler that clearly defines data protection expectations.

5. Town officials should ensure that PPSI found on the external hard drive is sanitized prior to sending the hard drive to the recycler for disposal.

6. Town officials should require employees to be trained on actions to take in the event of a data breach.

7. Town officials should regularly review the breach notification plan and ensure that key employees are aware of its provisions.

8. The Board should establish a comprehensive inventory policy that clearly defines its objectives concerning the duties, records and procedures required for protecting the Town's inventory of electronic equipment. The policy should:

   - Establish guidelines for maintaining records, physically securing assets and restricting access to and/or use of Town equipment, and document procedures governing the acquisition, transfer and disposal of such assets

   - Include a requirement for the reconciliation of disposal records to inventory.

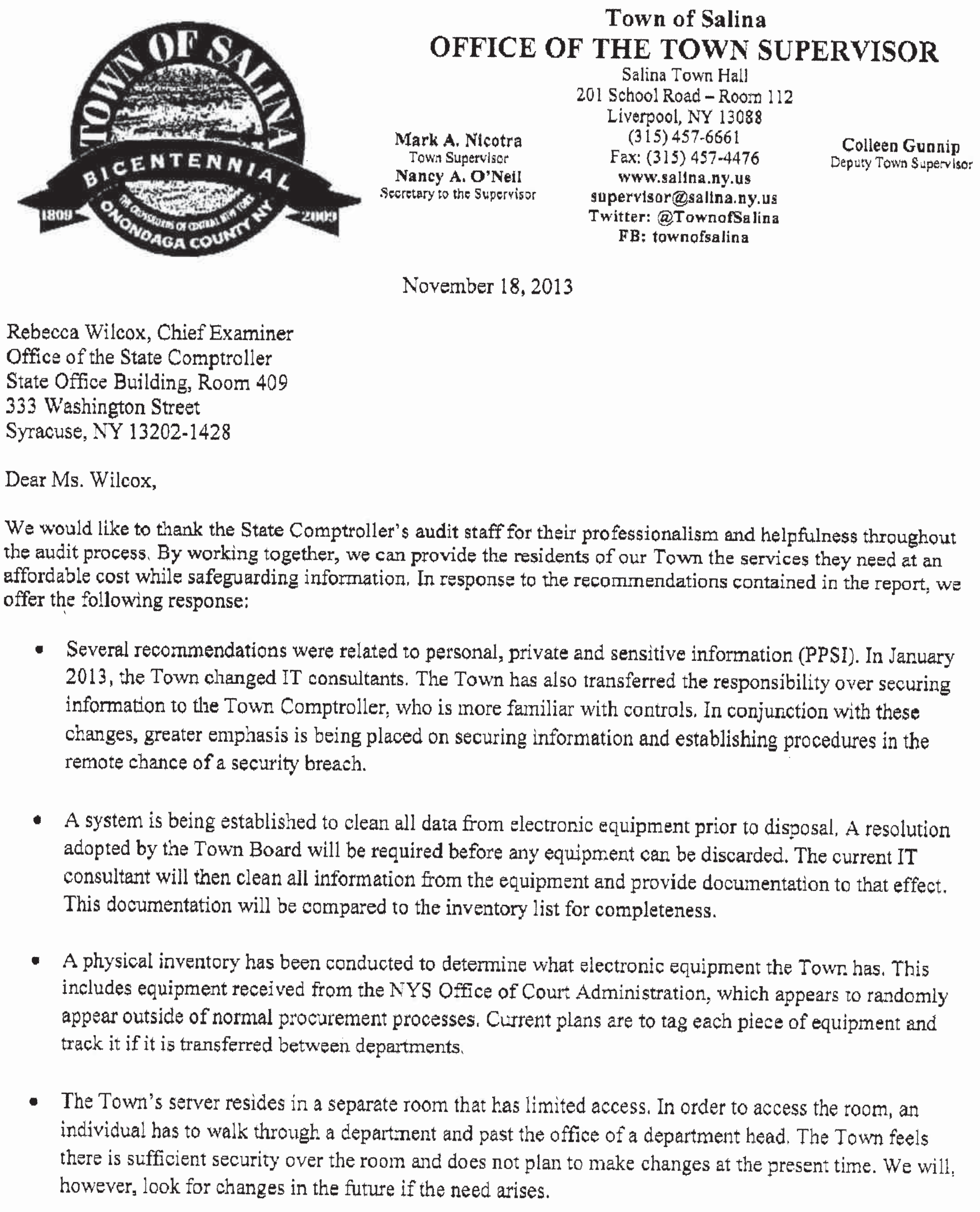
9. Town officials should implement physical security over the unlocked room containing the server and any other rooms with network access.

10. The Board should establish a formal disaster recovery plan that addresses the range of potential threats to the Town's IT systems and data and provides the guidance necessary to maintain Town operations or restore them as quickly as possible in the event of a disaster. This plan should be distributed to all responsible parties, periodically tested and updated as needed. Town officials should enter into a written agreement with any entities they plan on using for restoration of services.

APPENDIX A

RESPONSE FROM LOCAL OFFICIALS

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



Town of Salina

OFFICE OF THE TOWN SUPERVISOR

Salina Town Hall
201 School Road – Room 112
Liverpool, NY 13088
(315) 457-6661
Fax: (315) 457-4476
www.salina.ny.us
supervisor@salina.ny.us
Twitter: @TownofSalina
FB: townofsalina

Mark A. Nicotra
Town Supervisor
Nancy A. O'Neil
Secretary to the Supervisor

Colleen Gunnip
Deputy Town Supervisor

November 18, 2013

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

Dear Ms. Wilcox,

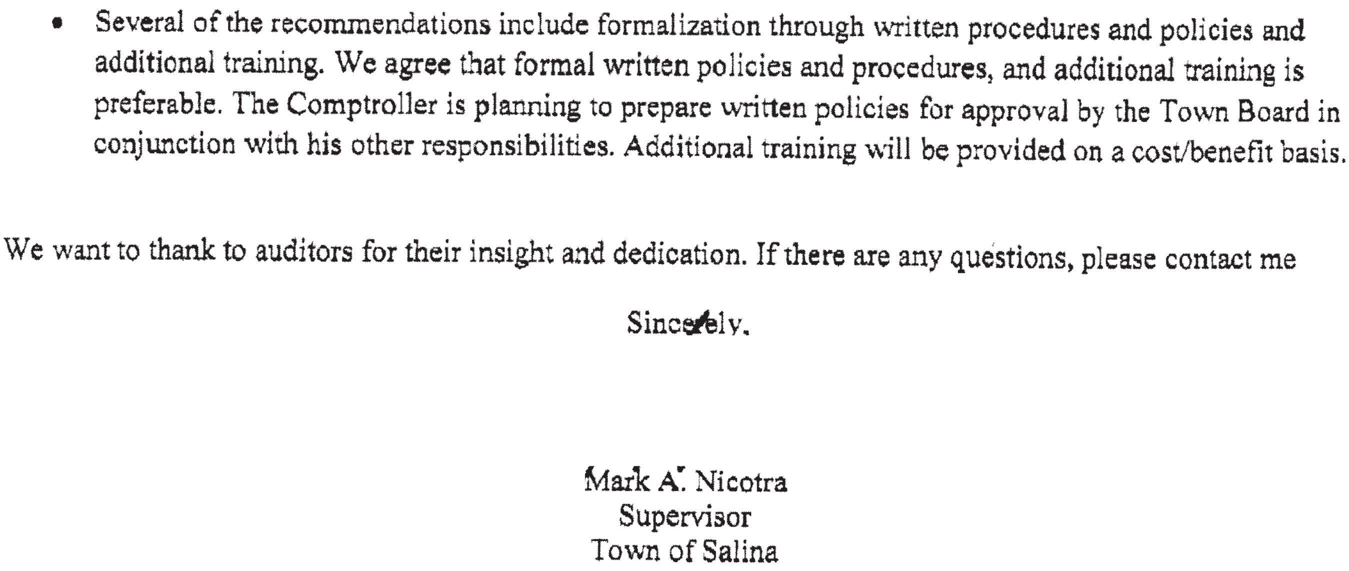
We would like to thank the State Comptroller's audit staff for their professionalism and helpfulness throughout the audit process. By working together, we can provide the residents of our Town the services they need at an affordable cost while safeguarding information. In response to the recommendations contained in the report, we offer the following response:

- Several recommendations were related to personal, private and sensitive information (PPSI). In January 2013, the Town changed IT consultants. The Town has also transferred the responsibility over securing information to the Town Comptroller, who is more familiar with controls. In conjunction with these changes, greater emphasis is being placed on securing information and establishing procedures in the remote chance of a security breach.

- A system is being established to clean all data from electronic equipment prior to disposal. A resolution adopted by the Town Board will be required before any equipment can be discarded. The current IT consultant will then clean all information from the equipment and provide documentation to that effect. This documentation will be compared to the inventory list for completeness.

- A physical inventory has been conducted to determine what electronic equipment the Town has. This includes equipment received from the NYS Office of Court Administration, which appears to randomly appear outside of normal procurement processes. Current plans are to tag each piece of equipment and track it if it is transferred between departments.

- The Town's server resides in a separate room that has limited access. In order to access the room, an individual has to walk through a department and past the office of a department head. The Town feels there is sufficient security over the room and does not plan to make changes at the present time. We will, however, look for changes in the future if the need arises.



- Several of the recommendations include formalization through written procedures and policies and additional training. We agree that formal written policies and procedures, and additional training is preferable. The Comptroller is planning to prepare written policies for approval by the Town Board in conjunction with his other responsibilities. Additional training will be provided on a cost/benefit basis.

We want to thank to auditors for their insight and dedication. If there are any questions, please contact me

Sincerely,

Mark A. Nicotra
Supervisor
Town of Salina

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

Our overall goal was to assess the adequacy of the internal controls put in place by officials to safeguard Town assets. To accomplish this, we performed an initial assessment of the internal controls so that we could design our audit to focus on those areas most at risk. Our initial assessment included evaluations of the following areas: control environment, financial condition, budgeting, accounting records and reports, cash management, cash receipts and disbursements, purchasing, claims processing, asset management, payroll and personal services, Town Clerk, real property taxes and information technology.

During the initial assessment, we interviewed appropriate Town officials, performed limited tests of transactions and reviewed pertinent documents, such as Town policies and procedures, Board minutes,and financial records and reports. In addition, we obtained information directly from the computerized financial databases and then analyzed it electronically using computer-assisted techniques. This approach provided us with additional information about the Town's financial transactions as recorded in its databases. Further, we reviewed the Town's internal controls and procedures over the computerized financial databases to help ensure that the information produced by such systems was reliable.

After reviewing the information gathered during our initial assessment, we determined where weaknesses existed and evaluated those weaknesses for the risk of potential fraud, theft and/or professional misconduct. Based on that evaluation, we determined that controls appeared to be adequate and limited risk existed in most of the financial areas we reviewed. We then decided on the reported objective and scope by selecting for audit the area most at risk: internal controls over information technology. To accomplish the objective of this audit and obtain valid audit evidence, our procedures included the following:

- We interviewed Board members, department heads, the former and current IT consultants, the Comptroller and the Deputy Comptroller.

- We obtained and reviewed Town policies and procedures related to IT.

- We tested multiple computers and servers by running audit software and examining temporary internet files, cookies and internet histories.

- We examined computer inventory records for March 24, 2010, June 1, 2012, and August 1, 2012, to determine the effectiveness of internal controls pertaining to electronic equipment inventories and any associated effects of deficiencies in those controls.

- We compared the 2010 inventory listing to the 2012 inventory listing to determine the number of computers and printers that were currently listed and those that were no longer listed.

- We determined the status of the computers no longer listed on the 2012 inventory listing.

- We reviewed computer disposal records for July 17, 2008, October 9, 2009, and March 8, 2012.

- We interviewed the maintenance worker who takes the old computer equipment to the recycler.

- We interviewed the recycler as to what its procedure is to sanitize computers.

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.

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
Nathaalie N. Carey, 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
Robert Meller, 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