DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2019M-125

Town of Haverstraw

Information Technology

DECEMBER 2019

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

Contents

Report Highlights

Town of Haverstraw

Audit Objective

Determine whether Town officials ensured the Town's Information Technology (IT) systems were adequately secured and protected against unauthorized use, access and loss.

Key Findings

- Employees accessed nonbusiness websites although it is prohibited by Town policy.
- Officials did not adopt a data classification, breach notification or online banking policy or a written disaster recovery plan.
- Employees were not provided with IT security awareness training.

In addition to this public report, sensitive IT control weaknesses were communicated confidentially to Town officials.

Key Recommendations

- Design, implement and enforce procedures to monitor the use of the Town's IT resources, including personal use.
- Adopt written IT policies and procedures to address data classification, breach notification, online banking and disaster recovery.
- Provide IT security awareness training to personnel who use IT resources.

Background

The Town of Haverstraw (Town) is located in Rockland County. The Town is governed by an elected Town Board (Board) composed of the Town Supervisor (Supervisor) and four Board members. The Board is responsible for the general oversight of Town operations and finances, including security over the Town's IT system.

The Town Supervisor (Supervisor) serves as the chief executive officer and is responsible for day-to-day operations.

The Town contracted with a third-party IT consultant to operate and maintain the Town's IT system. The Supervisor was responsible for overseeing the IT consultant.

Quick Facts	
Servers	3
Desktop and Laptop Computers	38
Employees	213
2019 General Fund Appropriations	$33 million

Audit Period

January 1, 2018 – January 22, 2019. We extended our scope period to February 28, 2019 for IT information collection.

Information Technology

How Does an Acceptable Use Policy Protect IT Assets?

A town should have an acceptable use policy (AUP) that defines the procedures for computer, Internet and email use. The policy also should describe what constitutes appropriate and inappropriate use of IT resources and the board's expectations concerning personal use of IT equipment and user privacy.

Monitoring compliance with AUPs involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity. Officials should monitor and analyze activities for signs of possible violations or imminent threats of violations of computer security policies, acceptable use policies or standard security practices.

Internet browsing increases the likelihood that users will be exposed to malware that may compromise data confidentiality, integrity or availability. Town officials can reduce the risks to personal, private and sensitive information (PPSI)[1] and IT assets by monitoring Internet usage and by developing and implementing procedures to ensure employee compliance with the AUP.

Internet browsing increases the likelihood that users will be exposed to malware that may compromise data confidentiality, integrity or availability.

Town Officials Did Not Enforce the Acceptable Use Policy

The Town had an AUP that defined proper procedures for using the Town's IT resources. However, Town officials did not design or implement procedures to monitor compliance with the policy or determine the amount of employees' personal use of Town computers.

We reviewed the web browsing history on 10 computers[2] and found questionable Internet use on three computers. This included social media use, personal shopping, accessing entertainment websites and web searches and browsing for non-Town related subjects. All three of the employees using these computers performed job duties that involved routinely accessing PPSI. As a result, their personal Internet use unnecessarily exposed this information to possibly being compromised.

Because the Town did not require officials to monitor employee Internet use, officials were unaware of this personal and inappropriate computer use. Town officials told us they did not design or implement procedures to monitor AUP compliance because they felt personal Internet use was not interfering with employee performance.

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

[2] Refer to Appendix B for information on our sample selection.

Internet browsing increases the likelihood of computers being exposed to malicious software that may compromise PPSI or expose the Town to ransomware attacks. As a result, the Town's IT assets and any PPSI they contain have a higher risk of exposure to damage and PPSI breach, loss or misuse.

What Other IT Policies and Procedures Should the Board Adopt?

To ensure the highest level of security over town data, the board should also adopt policies and procedures for data classification and the use of and access to PPSI. Data classification is the process of identifying data that contain PPSI to make informed decisions about how to properly protect it.

Officials should adopt a data classification policy to help ensure officials identify and organize Town data to determine what it is, where it is located and how to protect it. Furthermore, New York State Technology Law[3] requires local governments to adopt a breach notification policy that describes actions to be taken to notify affected individuals if PPSI is compromised.

In addition, the board should adopt an online banking policy to identify the online banking activities and electronic fund transactions that the Town may engage in; who is authorized to initiate, approve, transmit, record, review and reconcile online banking transactions; threshold amounts for these transactions; and required documentation to ensure security over Town funds. Officials should periodically review these policies, update them as needed and stipulate who is responsible for monitoring policy compliance.

The Board Did Not Adopt Sufficient IT Policies or Procedures

Although the Board adopted an AUP, it did not adopt written IT policies and procedures to address data classification and the use of and access to PPSI, breach notification and online banking. Town officials were unware of the requirement and need for these policies and procedures.

Without data classification and breach notification policies, officials could not ensure that employees were aware of their responsibilities for safeguarding sensitive information. Also, the Town may not be able to fulfill its legal obligation to notify affected individuals if this information is compromised.

Furthermore, because the Board did not establish an online banking policy, officials did not have procedures to identify approved online banking and electronic fund transfer activities, who was authorized to initiate and approve transactions and how to confirm, document, report and reconcile online activity.

[3] New York State Technology Law, Section 208

As a result, the Town had an increased risk that unauthorized individuals could access its bank account information and/or that fraud could occur and remain undetected.

Why Should the Town Manage User Permissions?

Network accounts enable the system to recognize specific users and grant authorized permissions to users. Officials are responsible for restricting user permissions to only those resources and data that are necessary for employees to perform their job functions. This helps ensure that PPSI is protected from unauthorized access and modifications and improves controls over financial transactions. A town should have a written policy and procedures for granting, modifying, revoking and periodically monitoring user permissions to the network and financial application software.

Officials Did Not Adequately Manage User Permissions

Town officials did not adequately manage user permissions to the Town's financial application. We reviewed six employees'[4] user permissions to the Town's financial application modules and found that two had excessive user permissions. The two employees were able to create, read, update and delete information from financial application modules without supervisory review. They did not need these user permissions to perform their job duties.

The Town did not have a written policy and officials did not develop procedures for managing, limiting and monitoring user permissions. Because officials did not periodically monitor user permissions, they were unware that the two employees had excessive user permissions to the financial modules. Employees with inappropriate user permissions to the Town's financial application could perform incompatible duties and make unauthorized changes without being detected.

Why Should the Town Have a Disaster Recovery Plan?

To minimize the risk of data loss or suffering a serious interruption of services, Town officials should establish a formal written disaster recovery plan (plan). This is particularly important given the current and growing threat of ransomware attacks. The plan should address the potential for sudden, unplanned catastrophic events (e.g., fire, flood, computer virus or inadvertent employee action) that could compromise the network and the availability or integrity of the financial system and any PPSI contained therein.

[4] See supra, note 2.

Typically, a plan involves analyzing business processes and continuity needs, focusing on disaster prevention and identifying roles of key individuals and necessary precautions to take to maintain or quickly resume operations. Additionally, a plan should include data backup procedures, such as ensuring a backup is stored off-site in case the building is destroyed or inaccessible, and periodic backup testing to ensure backups will function as expected.

Because computer viruses, such as ransomware, can be idle for a period of time before attacking an IT system, it is possible for recent backups to also contain viruses. Therefore, it is essential to have well-developed procedures for backing up and storing data.

The Board Did Not Adopt a Disaster Recovery Plan

The Board did not develop a formal written plan to establish how officials would respond to potential disasters. Consequently, in the event of a disaster, Town personnel have no guidance or plan to follow to restore or resume essential operations in a timely manner.

Although Town servers electronically backed up the Town IT system daily, officials did not develop written procedures to address who was responsible for ensuring backups were created successfully, how and how often backups should be created, how long backups should be retained, how often backups should be tested and where backups should be located and who should be responsible for their safety.

The Town's backups were stored on one of the servers and external hard drives located next to the domain controller.[5] Because backups were not stored in a secure offsite location, all network data could have been lost if attackers gained access to it, or if an environmental disaster occurred in the Town.

Town officials told us they were unaware of the need for a formal written plan. Without a formal written plan, the Town has an increased risk that it could lose important data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees, or process daily Town Clerk functions.

Why Should the Town Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, town officials should provide periodic IT security awareness training that explains the proper rules of behavior for using the Internet and IT systems and data. In

[5] The domain controller is the main server computer in the domain (network) that controls or manages all computers within the domain.

addition, training should communicate related policies and procedures to all employees.

The training should center on emerging trends such as information theft, social engineering attacks[6] and computer viruses and other types of malicious software, all of which may result in PPSI compromise or denying access to the IT system and its data. Training programs should be directed at the specific audience (e.g., system users or administrators) and include everything 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 or portable devices, such as thumb drives; the importance of selecting strong passwords; requirements related to protecting PPSI; risks involved with using unsecured Wi-Fi connections; or how to respond if a virus or an information security breach is detected.

Town Employees Were Not Provided With IT Security Awareness Training

The Town did not provide employees with IT security awareness training to help ensure they understand IT security measures necessary to protect the Town's IT system. Town officials told us that employees were required only to sign an acknowledgment form indicating they had read and understood the AUP. As a result, employees might not have been aware of risks associated with using the IT system and could have inadvertently exposed the Town's IT assets to cybersecurity attacks, loss and misuse.

The IT cybersecurity community identifies people as the weakest link in the chain to secure data and IT systems. District officials cannot protect the confidentiality, integrity and availability of data and computer systems without ensuring that users, and those who manage IT, understand the IT security policies and procedures and their roles and responsibilities related to IT and data security. Without periodic, formal 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. As a result, data and PPSI could be at greater risk for unauthorized access, misuse or abuse.

Each of the weaknesses discussed in this report exposed the Town to a risk of a data breach or compromise or malware, such as ransomware, that could deny access to the Town's IT system and data. However, it is important to note that there is a compounding effect of having multiple weaknesses. For example, lack of limits on Internet browsing makes users more likely to be attacked, lack of

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

training makes them more susceptible to the attacks and the lack of limits on user permissions increases the exposure from a successful attack. Given the current prevalence of ransomware attacks against municipalities, it is important for the Town to develop a comprehensive set of policies and procedures to protect its IT system.

What Do We Recommend?

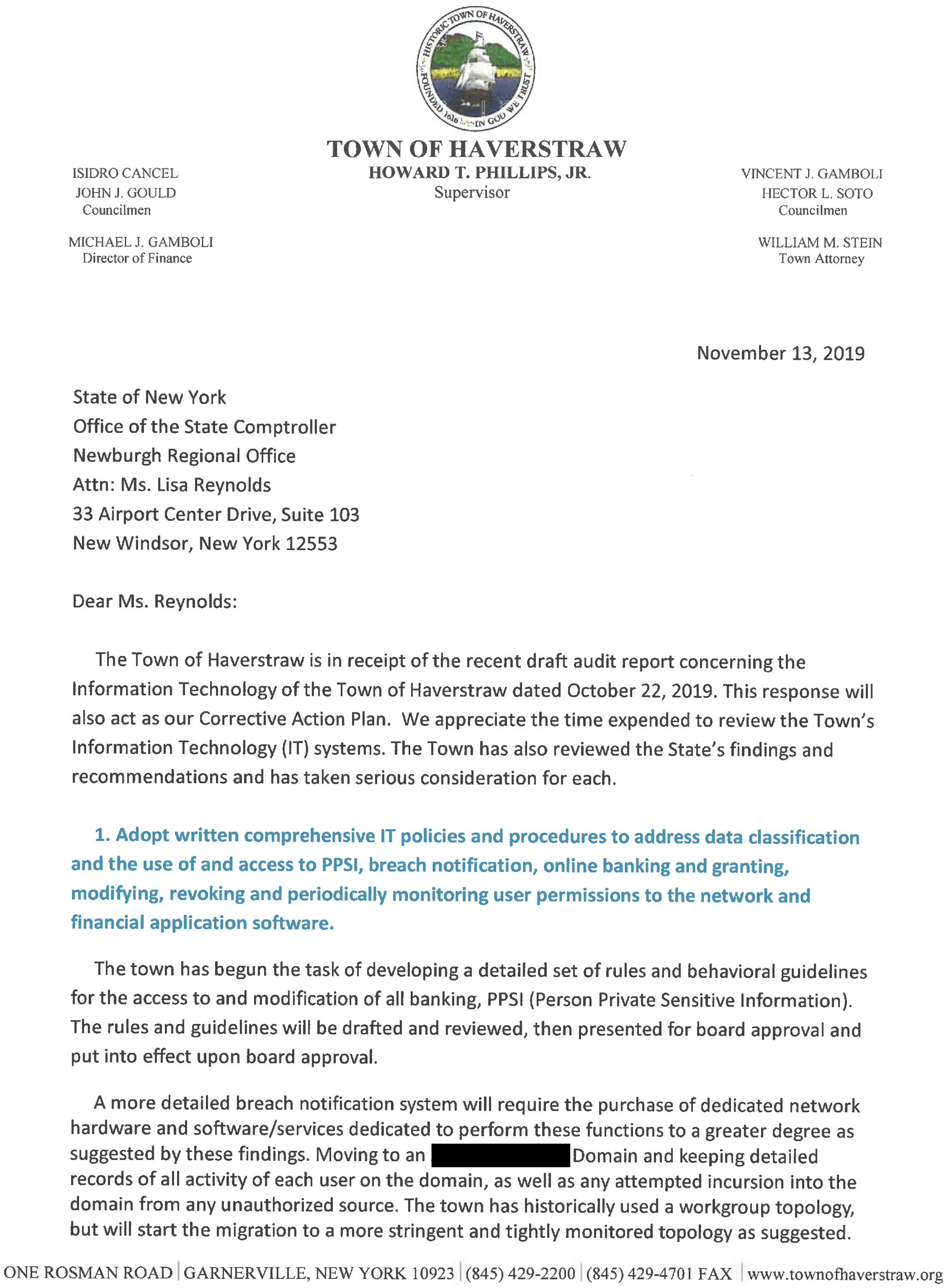
The Board should:

1. Adopt written comprehensive IT policies and procedures to address data classification and the use of and access to PPSI, breach notification, online banking and granting, modifying, revoking and periodically monitoring user permissions to the network and financial application software.

Town officials should:

2. Develop formal procedures for monitoring compliance with the AUP and all other IT policies.
3. Develop a formal, written disaster recovery plan.
4. Ensure data backups are stored at a secure offsite location.
5. Provide periodic IT security awareness training for Town employees.

Appendix A: Response From Town Officials



TOWN OF HAVERSTRAW

HOWARD T. PHILLIPS, JR.
Supervisor

ISIDRO CANCEL
JOHN J. GOULD
Councilmen

MICHAEL J. GAMBOLI
Director of Finance

VINCENT J. GAMBOLI
HECTOR L. SOTO
Councilmen

WILLIAM M. STEIN
Town Attorney

November 13, 2019

State of New York
Office of the State Comptroller
Newburgh Regional Office
Attn: Ms. Lisa Reynolds
33 Airport Center Drive, Suite 103
New Windsor, New York 12553

Dear Ms. Reynolds:

The Town of Haverstraw is in receipt of the recent draft audit report concerning the Information Technology of the Town of Haverstraw dated October 22, 2019. This response will also act as our Corrective Action Plan. We appreciate the time expended to review the Town's Information Technology (IT) systems. The Town has also reviewed the State's findings and recommendations and has taken serious consideration for each.

1. Adopt written comprehensive IT policies and procedures to address data classification and the use of and access to PPSI, breach notification, online banking and granting, modifying, revoking and periodically monitoring user permissions to the network and financial application software.

The town has begun the task of developing a detailed set of rules and behavioral guidelines for the access to and modification of all banking, PPSI (Person Private Sensitive Information). The rules and guidelines will be drafted and reviewed, then presented for board approval and put into effect upon board approval.

A more detailed breach notification system will require the purchase of dedicated network hardware and software/services dedicated to perform these functions to a greater degree as suggested by these findings. Moving to an [redacted] Domain and keeping detailed records of all activity of each user on the domain, as well as any attempted incursion into the domain from any unauthorized source. The town has historically used a workgroup topology, but will start the migration to a more stringent and tightly monitored topology as suggested.

After these topology and security changes are in place. all user permissions will be reviewed with the Supervisor and the Director of Finance on a regular basis, as well as whenever an employee for the Town of Haverstraw is hired, leaves employment or changes position going forward.

The town has also begun looking at deploying a completely separate network for internet access, making a physical break from all internal data and the internet. This would allow access to the internet without the risk of email, drive by, or other phishing type scams to result in the accidental exposure of data to these threats.

2. Develop formal procedures for monitoring compliance with the AUP and all other IT policies.

As stated above, with the implementation of new network topology and security measures, periodic activity checks on all employees (sites visited or attempted, use of internet and town email etc.), and reviews of all findings will be done with Supervisor and Director of Finance.

3. Develop a formal, written disaster recovery plan.

Although the town has a disaster recovery plan in place, which has been tested, it will be put into written form and submitted to the board and officially adopted. This will ensure a step by step procedure that could be followed by anyone qualified to do so in the event of an emergent situation.

4. Ensure data backups are stored at a secure offsite location.

This is being done already by the Director of Finance. Removable backups of all servers are taken off site by the Director of Finance daily. Going forward, a second, backup person will be assigned the duty if the Director of Finance is not able to do so for any reason (illness, vacation etc). Before backups are re-attached to the network, the responsible person will check to see that there has been no problem with the network overnight before attaching the drives to assure data remains unaffected in any case.

5. Provide periodic IT security awareness training for Town employees.

The Town of Haverstraw will start to provide Town employees IT security awareness training by use of webinars and NYS computer training materials on the NYS comptroller's website as well as using outside training resources to be chosen and deployed as we roll out safety modifications across the entire network, change network topology and begin implementation of suggested changes.

We would like to extend our appreciation for the cooperative effort to improve our Information Technology (IT) System and thank you for the State's recommendations made.

Sincerely,

Howard T. Phillips, Jr.
Town Supervisor

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 reviewed the Town's IT policies and procedures.
- We interviewed Town officials and the Town's IT contractor to gain an understanding of the Town's IT environment and internal controls.
- We reviewed user permissions for all six employees who used the Town's financial application to determine whether their user permissions were appropriate.
- We used our professional judgment to review 10 Town computers assigned to 10 employees who used the Town's financial application and/or could potentially access PPSI. The 10 computers had 11 local accounts. We ran a computerized audit script on the 10 computers and analyzed the data to determine whether Internet browsing histories contained personal use and/or high-risk activities.

Our audit also examined the adequacy of certain information technology controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to Town 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 Town Board to make the CAP available for public review in the Town 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