DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2020M-38

Greene County

Information Technology

SEPTEMBER 2020

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

Contents

Report Highlights

Greene County

Audit Objective

Determine whether officials ensured information technology (IT) systems were adequately secured and protected against unauthorized use, access and/or loss.

Key Findings

- County Legislators did not monitor compliance with the County's acceptable use policy, and did not adopt IT policies, including:
  - ○ Breach notification policy
  - ○ Disaster recovery plan
  - ○ Personal, private and sensitive information (PPSI) policy.
- County officials did not provide cyber security training to IT personnel and County employees.

Sensitive information technology (IT) control weaknesses were communicated confidentially to officials.

Key Recommendations

- Adopt comprehensive IT policies, communicate them to all employees, and review and update routinely or when significant changes in the environment occur.
- Provide adequate cyber security training to IT personnel and County employees.

County officials agreed with our findings and indicated they plan to initiate corrective action.

Background

The Greene County (County) Office Building is located in Greene County in the Town of Catskill. The County is governed by a 14-member Legislature, including a Chairman, Majority Leader and Minority Leader.

The County Administrator is appointed to execute the general management, supervision and direction of the County's day-to-day operations.

The County has two separate computer networks, one for the Sheriff's Department and one for the rest of the County. The County's IT Department, consisting of the Director and three staff members, is responsible for the maintenance of the County's networks, which have multiple servers and computers.

Quick Facts	
Number of Servers	29
Network User Accounts	471
2019 Budgeted Appropriations	$93.13 million

Audit Period

January 1, 2018 – October 4, 2019

Information Technology

What Are Effective Information Technology Controls?

The County's IT systems and data are valuable resources. The County relies on its IT systems for Internet access, email and for maintaining financial (and various other municipal) records. If the IT system is compromised, the results could be catastrophic and require extensive effort and resources to evaluate and repair. While effective controls will not guarantee the safety of a computer system, a lack of effective controls significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use. Acceptable use policies describe what constitutes appropriate and inappropriate use of IT resources, along with the Legislature's expectations concerning personal use of IT equipment and user privacy. The County's computer use and Internet policy prohibits the use of County computer systems for personal means. In addition, the County requires employees to sign acknowledgement forms to indicate they received the computer use policy to ensure employees are aware of and understand what is expected of them.

The County's acceptable computer use policy prohibits County employees from using County IT assets for any activities unrelated to department assignments and/or correspondence. Unacceptable computer use would include any illegal use, or any use for non-County business purposes. The acceptable use policy also prohibits viewing of inappropriate material such as pornography and gambling. In addition, the County's social networking policy indicates that personal social networking activities should only be done on personal time and only on personal equipment.

New York State Technology Law[1] requires municipalities to have a breach notification policy or local law that requires certain individuals to be notified when there is a system security breach involving private information. A disaster recovery plan provides a framework for reconstructing vital operations to resume time-sensitive operations and services after a disaster. Disasters may include any sudden, catastrophic event that compromises the availability or integrity of an IT system and data. Typically, a disaster recovery plan includes an analysis of business processes and continuity needs, disaster prevention instructions, specific roles of key individuals and precautions needed to maintain or quickly resume operations. The plan should be tested periodically and updated to ensure officials understand their roles and responsibilities in a disaster situation and to address changes in security requirements.

The County should develop and communicate written procedures for storing, classifying accessing, and disposing of personal, private, or sensitive information (PPSI).[2] This policy should define PPSI; explain the entity's reasons for collecting

[1] New York State Technology Law, Section 208

[2] PPSI is any information to which unauthorized access, disclosure, modification, destruction or disruption of access or use could severely impact critical functions, employees, third parties or citizens of New York in general.

PPSI; and describe specific procedures for the use, access to, storage and disposal of PPSI involved in normal business activities.

Officials should also develop comprehensive written procedures for managing system access that include periodic reviews of user access to ensure that user accounts are disabled when access is no longer needed.

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, County officials should provide periodic IT security awareness training that explains the proper rules of behavior for using the Internet and IT systems and data, and communicate related policies and procedures to all employees. The discussions could center on emerging trends in information theft and other social engineering[3] reminders; limiting the type of PPSI collected, accessed or displayed to that which is essential for the function being performed; malicious software; virus protection; the dangers of downloading files and programs from the Internet; passwords; Wi-Fi security; or how to respond if a virus or an information security breach is detected.

Officials Did Not Monitor Compliance With the Computer Use Policy

The County has a computer use policy in place and employees are required to sign acknowledgement forms indicating that they read and understood the policy. We reviewed 10 employee acknowledgement forms and found that two employees (20 percent) did not acknowledge the computer use policy. When policies are not clearly communicated, enforcement may be difficult. As a result of the policy not being communicated, employees may not understand the County's expectations for use of the County's computers.

Moreover, the County's acceptable computer use policy is outdated and inadequate. The policy has not been modified or updated to address the increased risks and changing concerns of the IT environment since its adoption in 2004. Failure to periodically revisit and update the acceptable computer use policy creates vulnerabilities and the policy may not address emerging IT security concerns. As a result, employees engaged in inappropriate computer use could expose the County's IT systems to vulnerabilities.

We also examined the website browsing history of 10[4] County computers and identified multiple instances of violations of the County's acceptable computer use and social networking policies. Review of web browsing history indicated employee access to prohibited sites, such as online shopping sites, personal

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

[4] See sampling methodology in Appendix B.

banking sites, personal email, social networking sites such as Facebook and Twitter, news sites, and entertainment sites such as YouTube.

We also reviewed the County's shared network folders to determine whether employees improperly used the network to store personal and/or inappropriate information. We detected multiple instances of the improper use of the County network's shared folders, including the storage of personal pictures such as wedding and vacation photos, as well as the storage of personal music files. The unauthorized use of County assets for prohibited use subjects County IT assets (and any PPSI contained on those assets) to a higher risk of exposure to misuse, loss and fraud. For example, personal files copied to the County's network could contain viruses or malware. Employees may be unaware of potential security threats the County is exposed to with inappropriate network and Internet usage.

The IT Director stated that there is no policy or stated procedure requiring him to periodically monitor or analyze website history logs. Periodic monitoring is not feasible because of limited IT personnel who are occupied with work orders from County individual computer users and departments. However, IT personnel could configure the web filtering software to generate a report to be sent periodically to department heads, who can monitor for compliance. In addition, the IT Director indicated that further web filtering restrictions were met with resistance from department heads, as certain departments require access to blocked sites to perform job duties. IT personnel may occasionally monitor a particular user, but only when a department head makes such a request. While the County does block access to certain websites, monitoring is still needed to ensure users cannot bypass those web filters.

Officials Did Not Adopt Adequate IT Security Policies

Breach Notification Policy – The Legislature and County officials have not developed and adopted a written breach notification policy. As a result, if PPSI is compromised, the County will not be appropriately prepared to fulfill its legal obligation to notify affected individuals. The County's IT Director stated that the required policy has not been adopted due to a lack of available resources, namely personnel, to devote the time required to develop it.

Use of, Access to, and Storage and Disposal of PPSI – The Legislature and County officials have not developed a classification scheme for PPSI or adopted a policy that identified the types of PPSI stored by the County, where the PPSI should be located, and who should have access to it. Unless officials classify the data they maintain and set up appropriate security levels for PPSI, there is an increased risk that PPSI could be exposed to unauthorized users, and effort to properly notify affected parties in the event of a data breach could be hampered.

In addition, County officials and employees may not understand what constitutes sensitive information and how to adequately safeguard it. In the event of a system compromise, officials may not be prepared to notify affected persons in a timely manner.

Disaster Recovery Plan − Officials have not developed a written disaster recovery plan to address potential disasters. Further, they have not formally identified, documented and prioritized essential systems and data. According to officials, the development of a disaster recovery plan has been delayed, in part, due to a lack of available resources, namely personnel. In addition, officials indicated that a lack of communications with department heads has stalled the development of a disaster recovery plan. It requires the cooperation of the IT personnel, department heads and County Legislature and officials to develop and execute an effective disaster recovery plan. Without a plan, in the event of a disaster, County officials have no guidelines to minimize or prevent the loss of equipment and data or to appropriately recover data vital for County government operations. Furthermore, essential employees may not be aware of their role, increasing the time and financial resources necessary to recover from the incident.

Officials Did Not Develop Procedures for Managing System Access

County officials have not developed comprehensive written procedures for managing system access for the County's 471 network user accounts. As a result, there is no formal process for notifying the IT department when an account should be disabled in the County's network. We examined the network for inactive user accounts.[5] We detected 43 inactive network user accounts which had not been disabled; the period of inactivity on the identified accounts ranged from two and a half months to 11.5 years. The IT Director indicated that all inactive user accounts were unnecessary, and all inactive accounts identified have since been disabled.

County officials did not establish formal procedures for reviewing network user accounts or disabling user accounts when employees separated from County employment. As a result, there is no process in place to inform the IT department when employees separate from employment. Further, unnecessary accounts create additional work to manage network access, along with the risk of errors that could result in users being inadvertently granted more access than needed.

Officials Did Not Provide IT Security Awareness Training

County officials did not provide IT personnel and users with IT security awareness training to help ensure they understand IT security measures designed to safeguard data from potential abuse or loss. The IT Director indicated that

[5] Inactive user accounts are accounts that have not logged into the network during a specified period of time.

cooperation from County officials is required to provide training to both IT personnel and network users.

The IT cybersecurity community identifies people as the weakest link in the chain to secure data and IT systems. County officials cannot protect the confidentiality, integrity and availability of data and computer systems without ensuring that users, or 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.

What Do We Recommend?

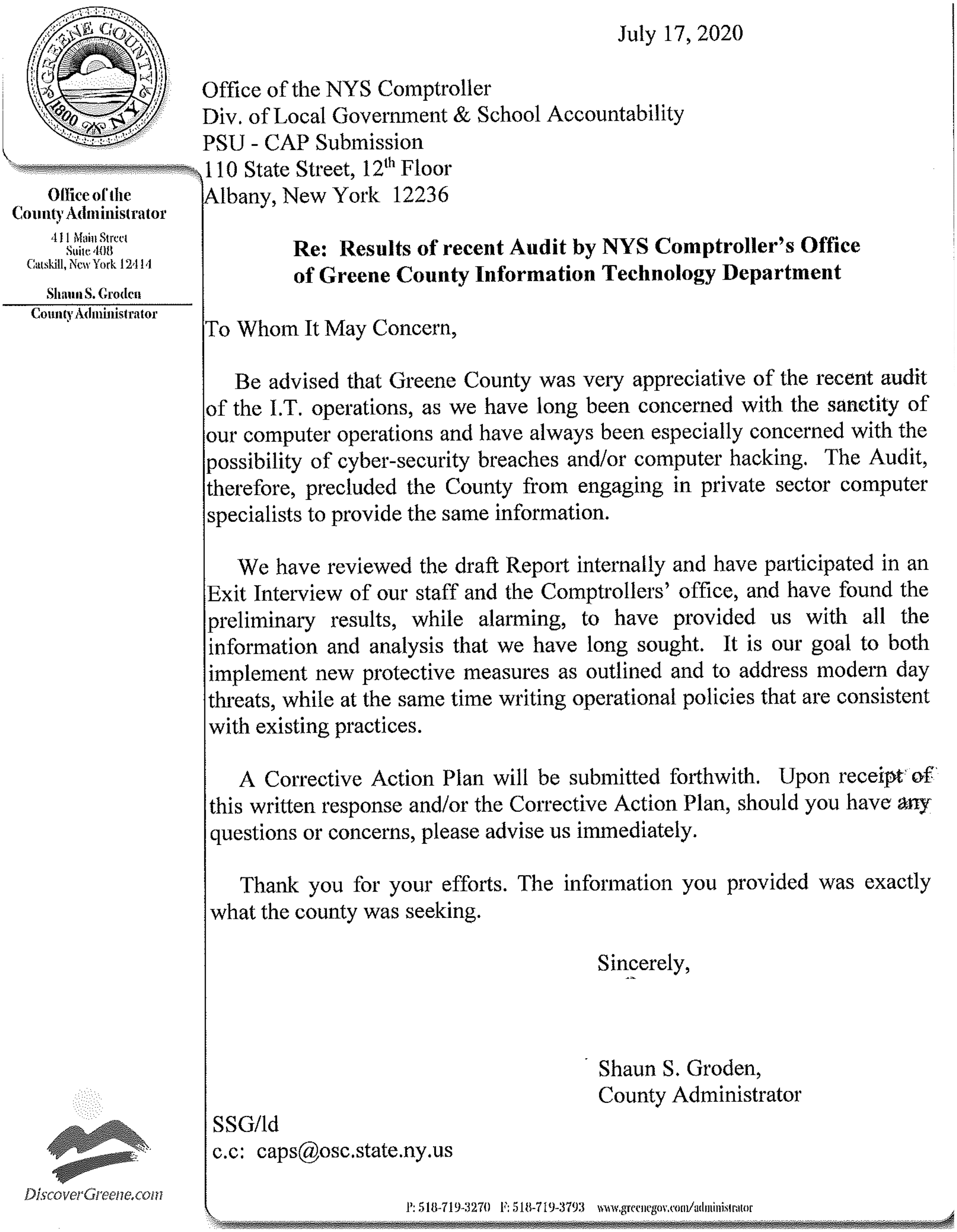
The Legislature should:

1. Update the acceptable use policy and communicate the policy to officials and employees.
2. Adopt comprehensive IT policies including a breach notification policy and personal, private and sensitive information policy.

County officials should:

3. Ensure the acceptable use policy is regularly reviewed, updated and distributed to users to obtain their written agreement of compliance with the policy terms.
4. Monitor users to ensure compliance with the acceptable use policies.
5. Develop a disaster recovery plan that identifies key personnel and test the plan to ensure it works as intended.
6. Develop written procedures for managing system access that include periodically reviewing user access and disabling user accounts when access is no longer needed.
7. Ensure that employees receive formal IT cybersecurity awareness training on an on-going basis that reflects current risks identified by the IT community.

Appendix A: Response From County Officials



Office of the
County Administrator

411 Main Street
Suite 408
Catskill, New York 12414

Shaun S. Groden
County Administrator

July 17, 2020

Office of the NYS Comptroller
Div. of Local Government & School Accountability
PSU - CAP Submission
110 State Street, 12th Floor
Albany, New York 12236

Re: Results of recent Audit by NYS Comptroller's Office of Greene County Information Technology Department

To Whom It May Concern,

Be advised that Greene County was very appreciative of the recent audit of the I.T. operations, as we have long been concerned with the sanctity of our computer operations and have always been especially concerned with the possibility of cyber-security breaches and/or computer hacking. The Audit, therefore, precluded the County from engaging in private sector computer specialists to provide the same information.

We have reviewed the draft Report internally and have participated in an Exit Interview of our staff and the Comptrollers' office, and have found the preliminary results, while alarming, to have provided us with all the information and analysis that we have long sought. It is our goal to both implement new protective measures as outlined and to address modern day threats, while at the same time writing operational policies that are consistent with existing practices.

A Corrective Action Plan will be submitted forthwith. Upon receipt of this written response and/or the Corrective Action Plan, should you have any questions or concerns, please advise us immediately.

Thank you for your efforts. The information you provided was exactly what the county was seeking.

Sincerely,

Shaun S. Groden,
County Administrator

SSG/ld
c.c: caps@osc.state.ny.us

DiscoverGreene.com

P: 518-719-3270 F: 518-719-3793 www.greenegov.com/administrator

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 Board minutes for resolutions concerning IT matters and reviewed written Board policies to determine the number and scope of policies officially adopted.
- We interviewed County officials and employees to obtain an understanding of IT operations.
- We reviewed County records for any IT-related policies and procedures.
- We performed a walk-through of the County to identify any weaknesses in the physical security controls over IT systems and devices and to obtain an understanding of the system's and their functionalities.
- We ran a computerized audit script on both of the County's domain controllers. We analyzed the report generated by the script, looking for any folders that could potentially contain PPSI. We also reviewed the report to identify any inappropriate use of shared folders on the County network, including the storage of personal files on the network.
- We reviewed County computers and inquired with employees to determine who had access to PPSI.
- We interviewed County employees to determine what safeguards were in place to protect sensitive data and financial assets.
- We used our professional judgment to select a sample of 10 County computers based on the type of work users performed and the likelihood that the user had access to PPSI. We reviewed web history reports for accessed websites that could put the network at risk.
- We used our professional judgment to select a sample of 10 County computers and ran a computerized audit script. We reviewed the results to determine the version of each software application, including operating system, installed on each computer.
- We reviewed the network user accounts and relevant security settings configured on both the County's and Sheriff's networks.

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 County 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.

Good management practices dictate that the Legislature has the responsibility to initiate corrective action. As such, the Legislature should prepare a plan of action that addresses the recommendations in this report and forward the plan to our office within 90 days.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/sites/default/files/local-government/documents/pdf/2018-12/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263196&issued=All

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263206&issued=All

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/sites/default/files/local-government/documents/pdf/2020-05/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/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263211&issued=All

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

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/local-government

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