Office of the New York State Comptroller

Division of Local Government
& School Accountability

Broome County

Information Technology

Report of Examination

Period Covered:

January 1, 2012 — August 20, 2013

2013M-351

Thomas P. DiNapoli

Table of Contents

		Page
AUTHORITY LETTER		2
INTRODUCTION		3
	Background	3
	Objective	3
	Scope and Methodology	3
	Comments of County Officials and Corrective Action	3
INFORMATION TECHNOLOGY		5
	Personal, Private and Sensitive Information (PPSI)	5
	Breach Notification Policy	6
	Disaster Recovery Plan	6
	Recommendations	7
APPENDIX A	Response From County Officials	8
APPENDIX B	Audit Methodology and Standards	11
APPENDIX C	How to Obtain Additional Copies of the Report	12
APPENDIX D	Local Regional Office Listing	13

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

May 2014

Dear County 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 County Legislature 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 Broome County, 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

Broome County (County) is located on the southern tier of New York State and covers 716 square miles. The County has approximately 200,000 residents. The County's budgeted expenditures for fiscal year 2013 totaled $247.7 million for the general fund. These expenditures were funded primarily with real property and sales taxes, State and Federal aid and user fees.

The County is governed by a 15-member County Legislature. The County Executive is the County's chief executive officer and is responsible, along with other administrative staff, for the County's day-to-day management. The County also uses the services of an Information Technology (IT) department which, under the supervision of the IT Director (Director), is responsible for all aspects of the County's data processing, programming, networking, software, computer and computer periphery acquisition and maintenance, as well as various communications responsibilities.

Objective

The objective of our audit was to determine if computerized data and assets were properly safeguarded. Our audit addressed the following related question:

- Did County officials ensure that computerized data and assets were properly safeguarded?

Scope and Methodology

We examined internal controls relating to the County's computerized data and assets for the period of January 1, 2012 through August 20, 2013. 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 County officials so they can 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 County Officials and Corrective Action

The results of our audit and recommendations have been discussed with County officials and their comments, which appear in Appendix A, have been considered in preparing this report. County officials agreed with our recommendations and indicated they planned to initiate corrective action.

The Legislature 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, R*esponding to an OSC Audit Report*, which you received with the draft audit report. We encourage the County Legislature to make this plan available for public review in the Clerk of the Legislature's office.

Information Technology

The County's IT system is a valuable and essential part of operations, 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 the County's computerized data is properly safeguarded. Accordingly, County officials are responsible for establishing internal controls over the IT system to ensure that County assets are protected against waste, loss and misuse. Among other things, IT controls should address the security of sensitive information. In addition, New York State Technology Law requires counties, cities, towns, villages and other local agencies to establish an information breach notification policy. Such a policy should detail how the local government would notify residents whose personal, private and sensitive information was, or is reasonably believed to have been, acquired by a person without a valid authorization. A system of strong IT controls includes a disaster recovery plan that describes how a local government will deal with potential disasters.

While the County does have certain IT user policies, they have not adopted a breach notification policy or a disaster recovery plan. As a result, there is an increased risk that computerized data could be lost or compromised or that County operations could be seriously disrupted.

Personal, Private and Sensitive Information (PPSI)

Local governments use and maintain data that contains PPSI. PPSI is any information where unauthorized access, disclosure, modification, destruction or disruption of access or use could severely impact the County's critical functions, employees, customers or third parties or the citizens of New York. For example, private information could include the following: Social Security number; driver's license number or non-driver ID; account number, credit card or debit card number and security code, access code or password that permits access to an individual's financial account. With the advancement of modern technology, the safeguarding of PPSI has become increasingly critical. Policies regarding the protection of PPSI should be developed and enforced by IT officials, including but not limited to the use of removable USB storage devices. If IT controls are unable to prevent the use of unauthorized or unencrypted storage devices, the risk to data security is significant.

We found that while the County does have a policy regarding USB removable media, they are not monitoring or enforcing the policy. County IT officials told us that each department has the ability to

order office supplies, including USB removable media on account. The IT Department does not have the capability to monitor or prevent unauthorized use of USB removable devices while still being able to allow authorized devices to operate. County IT officials also stated they did not aggressively monitor the use of USB media because it was determined that they are integral for some departments' operations.

IT officials must be diligent about understanding data security risks as well as taking appropriate steps to mitigate them. Securing technology equipment and electronic storage devices can prevent security breaches that can be very costly – not just financially, but also in terms of productivity losses, negative publicity, loss of PPSI and loss of residents' confidence.

Breach Notification Policy

An individual's private and/or financial information, along with confidential business information, could be severely affected if security is breached or data is improperly disclosed. New York State Technology Law requires counties, cities, towns, villages and other local agencies to establish an information breach notification policy. Such a policy should detail how the agency would notify residents whose personal, private and sensitive information was, or is reasonably believed to have been, acquired by a person without a valid authorization. It is important for the disclosure to be made expediently and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

While the Assistant IT Director provided us a draft policy, this draft had not been approved by the IT Department and was not adopted by the Legislature. By failing to adopt such a policy, in the event that private information is compromised, County officials and employees may not understand or be prepared to fulfill their legal obligation to notify affected individuals.

Disaster Recovery Plan

A disaster recovery plan provides a framework for reconstructing vital operations to ensure the resumption of time-sensitive operations and services in the event of an emergency. A strong system of internal controls includes a disaster recovery plan that describes how the County plans to deal with potential disasters. 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 the precautions to be taken to minimize the effects of a disaster and enable the County to either maintain or quickly resume critical functions. The plan should include a significant focus on disaster prevention and should be distributed to all responsible parties, periodically tested and updated as needed.

The County has not developed a formal disaster recovery plan to address potential disasters. Consequently, in the event of a disaster, County personnel have no guidelines or plan to follow to help minimize or prevent the loss of equipment and data or guidance on how to implement data recovery procedures. Further, without a disaster recovery plan, the County is at risk for the loss of important data and the disruption of time-sensitive operations.

Recommendations

1. The Director should safeguard PPSI by establishing procedures that more effectively monitor for, and prevent, the use of unauthorized and/or unencrypted portable storage devices.

2. County officials should develop a breach notification policy and a disaster recovery plan for resuming critical operations in the event of compromised PPSI information or a system failure.

APPENDIX A

RESPONSE FROM COUNTY OFFICIALS

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

Unit Name: Broome County Information Technology
Audit Report Title: Report of Examination
Audit Report Number: 2013M-351

Audit Response to Broome County IT Report Examination

Broome County agrees with the Audit Findings and Recommendations, noting the following:

Individual departments using their own Breach Notification Policy include: Broome County Health Department, Department of Social Services and Department of Mental Health.

The County Executive develops and recommends policies to be adopted by the County Legislature. Day to day management of the County is the County Executive's responsibility.

This Audit Response is also serving as the Corrective Action Plan.

Corrective Action Plan

Personal Private and Sensitive Information (PPSI)

Audit Recommendation:

- The Director should safeguard PPSI by establishing procedures that more effectively monitor for, and prevent, the use of unauthorized and/or unencrypted portable storage devices.

Implementation Plan of Action:

- We are currently looking at software to monitor and enforce policies regarding data loss prevention. We are in the proof of concept phase for this project.

Anticipated Implementation Date:

- 2nd Quarter of 2015.

Person Responsible for Implementation:

- Director of Information Technology.

Breach Notification Policy

Audit Recommendation:

- County officials should develop a breach notification policy for resuming critical operations in the event of compromised PPSI information or a system failure.

Implementation Plan of Action:

- We have a rough draft to this policy. This is included in our Security Policy for Broome County. This is about 30 days from being complete to submit to legal for review, then legislature for approval.

Anticipated Implementation Date:

- 3rd Quarter of 2014.

Person Responsible for Implementation:

- Director of Information Technology.

Disaster Recovery Plan

Audit Recommendation:

- County officials should develop a disaster recovery plan for resuming critical operations in the event of compromised PPSI information or a system failure.

Implementation Plan of Action:

- Emergency Services has submitted a Request for a Consultant to help with the building stages of the Disaster Recovery.

Anticipated Implementation Date:

- 3rd Quarter of 2015.

Person Responsible for Implementation:

- Broome County Executive's Office, Broome County Information Technology Department.

Signed:

Debra A. Preston

Name

5/5/14

Date

Broome County Office Building . 60 Hawley Street . P.O. Box 1766 . Binghamton, New York 13902
Phone: (607) 778-2200 . Fax: (607) 778-6132 . www.gobroomecounty.com

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

During this audit, we examined the County's IT system. To accomplish our audit objective and obtain relevant audit evidence, our procedures included the following:

- We conducted in-person interviews with various County officials and employees to gain an understanding of the controls over the IT system.

- We inspected and observed County operations regarding the County's IT hardware and software.

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
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
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