



Town of Fort Edward

Accounting Records and Information Technology

Report of Examination

Period Covered:

January 1, 2010 — December 31, 2011

2012M-101



Thomas P. DiNapoli

Table of Contents

	Page
AUTHORITY LETTER	2
EXECUTIVE SUMMARY	3
INTRODUCTION	5
Background	5
Objective	5
Scope and Methodology	5
Comments of Local Officials and Corrective Action	6
RECORDS AND REPORTS	7
Accounting Records	7
Financial Reporting	8
Recommendations	9
INFORMATION TECHNOLOGY	10
IT Policies and Security Awareness	10
Contracts with Third Parties	12
Recommendations	13
APPENDIX A Response From Local Officials	14
APPENDIX B Audit Methodology and Standards	16
APPENDIX C How to Obtain Additional Copies of the Report	18
APPENDIX D Local Regional Office Listing	19

State of New York Office of the State Comptroller

Division of Local Government and School Accountability

September 2012

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 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 Fort Edward, entitled Accounting Records and 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*



State of New York Office of the State Comptroller

EXECUTIVE SUMMARY

The Town of Fort Edward (Town) is located in Washington County. The Town provides services that include street maintenance, snow plowing, and general government administration. The Town is governed by a Board that is comprised of an elected Town Supervisor and four elected councilpersons. The Supervisor serves as the chief executive officer, chief fiscal officer, and budget officer.

The 2011 budget for the town-wide general fund totaled \$913,349, the part-town general (area outside the Village) fund was \$92,746 and the highway fund was \$606,900. The adopted budget for 2012 totaled approximately \$1,584,000 for the same three funds. The Town's expenditures were funded primarily with revenues from real property taxes, local fees, and State aid.

Scope and Objective

The objective of our audit was to review the Town's accounting records and reports and information technology policies for the period January 1, 2010 to December 31, 2011. Our audit addressed the following related questions:

- Did the Town maintain adequate records to accurately and reliably account for and report on its financial activities?
- Did the Board adequately design and implement policies over the security of information technology that ensure the protection of the Town's IT assets and data?

Audit Results

The Town's annual financial reports (AUD) filed with OSC contained inaccuracies, some of which apparently persisted for several years. These inaccuracies were carried forward from the 2010 fiscal year into the 2011 fiscal year even after the Town hired an accountant to reconcile and had not been corrected as of the end of 2011. The Town has filed the required AUD significantly late every year from 2007 through 2010 ranging from 173 days to 293 days late.

The Town did not establish written information technology policies to address acceptable computer use and provide security awareness to computer users in both the Town and Village who access the network. The Town did not establish a disaster recovery plan or a breach notification policy as required by law. Additionally, a service agreement that the Town entered with an outside technology services provider included vague language that did not adequately describe the services that the Town was due to receive.

Comments of Local Officials

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

Introduction

Background

The Town of Fort Edward (Town) is located in Washington County. According to 2010 United States Census data, the Town has a population of about 6,400, an increase of about 8 percent from the 2000 census. The Town is governed by a Board that comprises a Town Supervisor (Supervisor) and four Councilpersons. The Supervisor serves as the chief executive officer, chief fiscal officer, and budget officer. The Supervisor has a part-time account clerk who assists him with these responsibilities by maintaining the Town's accounting records. The Town obtained an annual independent audit by a CPA for the 2010 fiscal year and engaged the same CPA to audit the Town's financial records for the 2011 fiscal year.

The 2011 budget for the town-wide general fund, the part-town general (area outside the Village) fund, and the highway fund totaled \$1,612,995, and the adopted budget for 2012 totaled approximately \$1,584,000 for the same three funds. The Town's expenditures were funded primarily with revenues from real property taxes, local fees, and State aid.

The Town provides limited services that include street maintenance, snow plowing, and general government administration. The Town shares a building with the offices of the Village of Fort Edward (Village). To limit costs, the Town and Village share the costs of building maintenance and share a computer network. The Town is responsible for the network's physical security and maintenance.

Objective

The objective of our examination was to evaluate the Town's accounting records and reports and information technology policies. Our audit addressed the following questions:

- Did the Town maintain adequate records to accurately and reliably account for and report on its financial activities?
- Did the Board adequately design and implement policies over the security of information technology that ensure the protection of the Town's IT assets and data?

Scope and Methodology

We examined accounting records and reports and the information technology policies of the Town of Fort Edward for the period January 1, 2010 to December 31, 2011.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such

standards and the methodology used in performing this audit are included in Appendix B of this report.

**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 initiate corrective action.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and forwarded to our office within 90 days, pursuant to Section 35 of 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. The Board should make this plan available for public review in the Town Clerk's office.

Records and Reports

The Supervisor, as the Town's chief fiscal officer, is responsible for maintaining complete, accurate, and up-to-date accounting records. These records provide the basis for periodic reports to the Board and the annual update document (AUD), the Town's annual financial report. Article 3 of General Municipal Law requires municipalities to file the AUD with the Office of the State Comptroller (OSC) following the close of the fiscal year. The Board must provide for an annual audit of the Supervisor's financial records and reports to fulfill its fiscal oversight responsibilities.

We found that the Town properly recorded revenues and expenditures, and that Town records of revenues and expenditures agreed with both the audited financial statements and the AUD for 2010.¹ However, numerous balance sheet accounts contained inaccuracies, some of which have been carried forward from prior years, and have not been corrected. Having inaccurate accounting records makes it difficult for the Board to monitor the Town's financial condition, and difficult to file the AUD on time. In fact, the Town has filed the AUD late every year from 2007 through 2010. Despite the errors in its balance sheet accounts, the Town has so far been able to manage its finances. However, going forward, it is essential that Town officials correct the accounting records to provide the Board with accurate information about the Town's financial condition, and file the Town's AUD in a timely manner.

Accounting Records

Accounting records are used to measure a government's financial condition, determine the results of operations, and serve as a basis for numerous decisions that management makes concerning government operations. To be useful, accounting records need to be accurate, complete and up to date. Accounting records are also the basis for, and should agree with, the AUD that is filed by the Town and used by the Board.

We examined the Town's cash receipt and disbursement recording procedures and found they were adequate, and that accurate revenue and expenditure information was recorded in the accounting records. For example, we tested approximately \$96,000 in garbage sticker sales and more than \$6,000 of building permits for the 2011 fiscal year. Except for minor exceptions that we discussed with management, we found that they were accurately recorded, reported, and deposited

¹ The Town filed its 2010 AUD on September 30, 2011 (183 days late). The Town has not yet filed its AUD for 2011 or requested an extension for filing

timely and intact. We also reviewed 20 disbursements totaling about \$77,000. We found they were adequately documented, and correctly recorded in the accounting records. We also traced from the 2010 audited financial statements to the AUD, and from the AUD to the Town's accounting records and found that, except for minor differences, the amounts for revenues and expenditures reported on the AUD agreed with both the Town's financial records and the audited financial statements.

We also tested 100 percent of the balance sheet accounts (assets, liabilities, and equity or fund balance) for the general, part-town general, and part-town highway funds, including inter-fund loans from the general fund to other funds. We found numerous discrepancies between the 2010 AUD, which was based on the audited financial statements, and the Town's accounting records for certain balance sheet accounts in all three funds. The discrepancies exist because Town officials did not make any adjustments to correct the errors and discrepancies found by the CPA in the accounting records.² Many of the errors we identified in the 2010 balance sheet carried forward into the 2011 fiscal year. The account clerk acknowledged these discrepancies and said that he has asked the Town's CPA to help make audit adjustments that will correct the balance sheet account errors.

Having accounting records that do not agree with the AUD makes it difficult for the Board to monitor the financial condition of the Town. Because of the Town's small budget, its generally accurate accounting for cash receipts and disbursements, and the Board's periodic budget monitoring, Town officials have been able to conduct Town financial operations and prepare budgets, despite the errors in its accounting records. However, the Town should ensure that its accounting records are corrected to ensure that they reflect the Town's true financial position and agree with the Town's AUD.

Financial Reporting

The Town is required to annually file an AUD with OSC within 90 days from the close of its fiscal year. In the event that the Town anticipates missing the deadline, Town officials can request an extension that allows the Town up to 120 days to file the report.

In recent years, the Town's financial reports have been significantly late: specifically, the Town's AUD was filed 175 days late in 2007, 173 days late in 2008, and 293 days late in 2009. The Supervisor explained that the Town's late submissions for 2007 and 2008 occurred because a prior accountant, whom the Town had paid to file the AUDs, had filed them late.

² The Town hired a certified public accountant (CPA) to audit the Town's accounting records for the 2010 fiscal year and to help prepare the AUD.

To improve timeliness, the Supervisor hired the Town's current CPA to prepare and submit the report for 2009. According to the Supervisor, the CPA took a significant amount of time to prepare the report due to the condition of the Town's financial records. The same CPA was engaged to audit the financial records and prepare the annual reports for the 2010 and 2011 fiscal years. For the 2010 fiscal year, the CPA again required additional time to produce audited financial statements and prepare the AUD because of continuing errors in balance sheet accounts, along with other errors that occurred because of the software conversion. As a result, the 2010 AUD was due on May 1, 2011, but was not filed until September 30, 2011. As of the time we completed field work, the Town had not yet filed the AUD for 2011, and had not requested an extension. Correcting the errors in the Town's balance sheet accounts should enable Town officials to file their AUD on time.

Recommendations

1. The Supervisor and Account Clerk should ensure that all necessary audit adjustments are made to correct the accounting records and support the Town's AUD.
2. The Supervisor should continue efforts to ensure that the Town submits the AUD on time.

Information Technology

The Town relies on its IT system to perform a variety of tasks including bookkeeping and accounting, word processing, email communication, Internet access, online banking, and reporting to State and Federal agencies. Information and data related to finances, payrolls, and general Town government business are stored on the IT network's single server. Additionally, to save operating costs, the Town and Village of Fort Edward share networking resources. This arrangement is also logistically convenient because the two local governments occupy the same building. The Town uses three computers and the Village uses two that are networked and all share the same server. The Town assumes overall responsibility for maintaining the network. These responsibilities include obtaining technical support, physically securing the networking components, and backing up the data that are stored on the network server, which is located in the Supervisor's office.

By adequately preventing unauthorized access to its IT systems and data, the Town can reduce the risks that computer equipment could be damaged, or that electronic data could be misused, lost, or corrupted without detection. Even small disruptions in the IT system can require extensive time and effort to evaluate and repair. Town officials are responsible for designing and implementing a comprehensive system of internal controls over IT to protect these assets from unauthorized or inappropriate use. Both administrative and information system controls should be part of any IT security system. This is especially important because of the increasing use of viruses, malware,³ and other virulent methods intended to harm data resources and gain unauthorized access to valuable data.

IT Policies and Security Awareness

Effective protections of computing resources and data include an acceptable use policy that informs users about appropriate and safe use of Town computers, security awareness training, a breach notification policy that identifies actions to take if personal and confidential information is released to unauthorized parties, and a disaster recovery plan with guidance for minimizing loss and restoring operations should a disaster occur.

³ Malware, or malicious software, consists of programming designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, or otherwise cause damage. A computer worm is a self-replicating malware computer program which uses a computer network to send copies of itself to other computers on the network.

An acceptable use policy defines the Board's intended use of equipment and computing software, and the security measures that are designed to protect the Town's network and confidential information. The policy should address, but not necessarily be limited to, the acceptable use of the Internet, email, password security, access to and use of confidential information, and the installation and maintenance of software on Town computers.

Computer users also need to be aware of security risks and properly trained in practices that reduce the internal and external threats to the network. An effective IT policy includes provisions for the monitoring of computer use to ensure compliance, as well as provisions for policy enforcement. Computer system users should provide written acknowledgement that they are aware of, and will abide by, the IT policies. The implementation of effective IT policies and practices facilitates the protection of computerized data resources from internal and external threats. The Town should ensure that all network users, both Town and Village employees, are sufficiently trained in proper and secure use of the shared computing resources.

Further, the State Technology Law requires local governments to establish an information breach notification policy. The policy should detail how employees would notify State residents whose private information was, or is reasonably believed to have been, acquired by a person without a valid authorization. The disclosure should be made in the most expedient time possible 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.

It is also essential that Town officials develop a formal disaster recovery plan that addresses the range of threats to their IT system. The plan should focus on sustaining the entity's critical business functions during and after a service disruption (for example, an extended power outage or a fire in the municipal building). It is important that Town officials analyze data and operations to determine which are the most critical and what resources are needed to recover and support these operations in the event of an emergency. Once the disaster recovery plan is finalized, Town officials should distribute it to all responsible parties, periodically test procedures to make sure they work as intended, and update the plan as needed.

The Town did not establish written policies for acceptable computer use to define the Board's intentions for use of Town computer equipment. The lack of such a policy significantly increases the risks that hardware and software systems and the data they contain may be lost or damaged by inadvertent accidents or deliberately malicious

exploits. This leaves the Town vulnerable to the risks associated with individual use, including computer viruses, spyware, and other forms of malware that could potentially be introduced if employees access non-work-related websites or download unauthorized programs.

We also found that the Town did not provide security awareness training to users to make sure they understand security measures designed to protect the Town's network and confidential information. For example, while we were on site, we observed that the network's anti-virus software was about two months out of date. Although the software was flashing a warning message, Town employees we spoke to said they did not know who was supposed to be monitoring the anti-virus software and initially did not know how to respond to the warning message. A Village user told us that she turns off pop-up messages concerning updates to the internet browser because she does not know what to do about them. The Town's IT assets are more vulnerable to loss and misuse when network users are not aware of security risks and practices needed to reduce those risks.

We also found that the Town had not developed a breach notification policy, as required by law. The lack of such a policy potentially delays the communication of compromised information to the necessary parties involved. The Town also lacks a formal disaster recovery plan to address potential disasters. Consequently, in the event of a disaster, Town 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. Without a disaster recovery plan, the Town is at risk for the loss of important data and the disruption of time-sensitive operations.

Contracts with Third Parties

Many local governments do not employ staff with sufficient expertise to service all the hardware and software components of a computer networking system. Therefore, they rely on the services that are provided by outside IT vendors that may include various forms of technical support and services for hardware and software.

To avoid potential misunderstandings, local governments should have written agreements with computing service providers that address the local government's needs and expectations, and specify the level of service to be provided by the independent contractor/vendor. The provisions of such an agreement would generally include an identification of the parties to the contract; definitions of terminology; the duration of the agreement; the scope and type of services to be provided; limitations (what, if anything, is excluded); service objectives and indicators of performance; roles and responsibilities of all parties; the impact of nonperformance; pricing, billing and terms of payment; security procedures; reviews and updates to the

terms. The more specific the agreement is, the better: there should be no uncertainty about what the contractor will provide, when it will be delivered, and how much the item or service will cost. An agreement that lacks specificity can lead to additional costs or cost increases the local government was not expecting.

The Town entered into four agreements with vendors for various services that include software service and support, online banking, and network services. While three of the four agreements explain the technical services, roles of the parties, service limitations, and cost of services, the Town's agreement with one service provider was a one-page document that did not specify the services the Town was paying for. This agreement states that the vendor provides on-site service, telephone service, and emergency service, and includes a breakdown of service charges and billing terms. However, the document did not specify the actual services the vendor was providing, the roles and responsibilities of the parties, and what components of the Town's computer network are covered. Additionally, the document expired as of May 12, 2011.

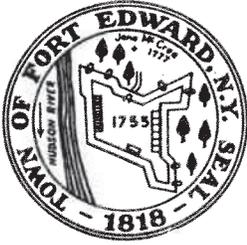
Town officials told us that this vendor is providing important network services that include critical hardware and software support (e.g., anti-virus and anti-spam software, a firewall, intrusion detection, and server support). Given the essential nature of these services, the Town needs to have a current written agreement with its vendor that clearly explains the expectations, roles, and responsibilities of the parties to ensure Town systems and data are protected and supported. Although the vendor has continued to provide services to the Town according to the terms of the expired agreement, the Town should have current contracts with all its service providers.

Recommendations

3. The Board should establish information technology policies that address acceptable use, security awareness, and breach notification. The Board should ensure that employees are aware of and comply with these policies.
4. The Board should establish a disaster recovery plan.
5. The Board should ensure that all agreements with vendors providing technology services clearly explain what services they are providing, and the roles and responsibilities of all parties. The agreements should be current and up-to-date.

APPENDIX A
RESPONSE FROM LOCAL OFFICIALS

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



TOWN OF FORT EDWARD

118 BROADWAY

P.O. BOX 127

FORT EDWARD, N.Y. 12828-0127

Dear Comptrollers Office:

Please be advised the Town Supervisor and the Town Board have reviewed the Accounting Records And Information Technology Audit. We are preparing the Corrective Action Plan. We have received information from several agencies in regards to Computer use and security. Myself and my Account Clerk have reviewed the entries that need to be made and with help from our CPA the proper adjustments will be made.

The Corrective Action Plan will be submitted within the 90-day period.

Sincerely,

Mitchell C. Suprenant
Supervisor
Town of Fort Edward

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 and monitor financial activities. 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.

During the initial assessment, we interviewed Town officials, performed limited tests of transactions, and reviewed pertinent documents such as Town policies, Board minutes, and financial records and reports. 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. We then decided upon the reported objective and scope by selecting for audit those areas most at risk. We selected accounting records and information technology for further audit testing.

To review the Town's accounting system and records we performed the following steps.

- We interviewed officials to gain an understanding of the Town's budgeting process and accounting system.
- We reviewed the results of operations and compared the audited financial statements to the annual update document and the Town's general ledger.
- We compared the adopted budgets to the accounting records.
- We assessed the composition of significant balance sheet accounts.
- We reviewed the periodic reports prepared by the Town Supervisor and the Town Clerk.
- We analyzed inter-fund loans.
- We reviewed budget amendments, Board meeting minutes, and resolutions.
- We selected and reviewed samples of cash receipts and cash disbursements.
- We reviewed bank statements and bank reconciliations to the accounting records.
- We tested the reliability of the data maintained on the accounting system.

To review the Town's information technology network we performed the following steps.

- We interviewed Town officials and reviewed documentation to determine existing policies related to the use of information technology and cyber-security awareness.

- We interviewed computer users and asked them to demonstrate their normal procedures for opening programs, accessing and browsing the internet, and accessing email and online bank accounts.
- We also interviewed computer users to assess their general knowledge of cyber-security awareness.
- We reviewed the Town's written agreements with outside parties who provide information technology services.
- We contacted the owner of a vendor providing technology services to obtain information about the services.

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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

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
Steven J. Hancox, 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-Bufferalo@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
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

Christopher Ellis, 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 AND REGIONAL PROJECTS

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