



Geneseo Central School District Information Technology

Report of Examination

Period Covered:

July 1, 2006 — February 1, 2008

2008M-153



Thomas P. DiNapoli

Table of Contents

	Page
AUTHORITY LETTER	2
INTRODUCTION	3
Background	3
Objective	3
Scope and Methodology	3
Comments of District Officials and Corrective Action	4
INFORMATION TECHNOLOGY	5
District-Wide Security Plan	5
Disaster Recovery Plan	6
Flash Drives	6
Recommendations	7
APPENDIX A Response From District 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

November 2008

Dear School District Officials:

A top priority of the Office of the State Comptroller is to help school district officials manage their districts efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support district operations. The Comptroller oversees the fiscal affairs of districts statewide, as well as districts' 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 district operations and Board of Education governance. Audits also can identify strategies to reduce district costs and to strengthen controls intended to safeguard district assets.

Following is a report of our audit of the Geneseo Central School District, 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 district officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

*Office of the State Comptroller
Division of Local Government
and School Accountability*

Introduction

Background

The Geneseo Central School District (District) is located in the Towns of Geneseo, Groveland, Sparta and West Sparta, Livingston County. The District is governed by the Board of Education (Board) which comprises seven elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer of the District and is responsible, along with other administrative staff, for the day-to-day management of the District under the direction of the Board.

There is one school in operation within the District, with approximately 975 students. The District's budgeted expenditures for the 2007-08 fiscal year were approximately \$16 million, which were funded primarily with real property taxes and State and Federal aid.

The Technology Coordinator, in conjunction with a part-time Computer Services Assistant employed by Educational Technology Services (Edutech),¹ is responsible for the day-to-day management of the District's information technology systems. The District's current computer system is a networked system (wired and wireless access) which consists of workstations (desktop and laptop) located in computer labs, media centers, classrooms, Business Office, and conference and faculty rooms.

Objective

The objective of our audit was to assess internal controls over information technology functions. Our audit addressed the following related questions:

- Does the District have a written District-wide security plan?
- Is the District's disaster recovery plan adequately designed so that the District can continue operations if a disaster occurs?
- Are flash drives issued by the District properly secured?

Scope and Methodology

We examined the District's internal controls over information technology for the period July 1, 2006 to February 1, 2008.

¹ The Genesee Valley/Wayne Finger Lakes Educational Technology Services (EduTech) is a Regional Information Center that provides technology services to school districts in New York State.

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 District
Officials and Corrective
Action**

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

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of the GML, Section 2116-a (3)(c) of the Education Law and Section 170.12 of the Regulations of the Commissioner of Education, a written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and forwarded to our office within 90 days. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. 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 the CAP available for public review in the District Clerk's office.

Information Technology

District management relies on its information technology (IT) system to maintain financial and student data, process financial transactions, provide computer education, access the Internet, communicate by electronic mail (e-mail), and to report to State and Federal agencies and the general public. The potential consequences of a system failure can range from inconvenient to severe; even small disruptions in processing can require extensive time and effort to evaluate and repair. Computerized personal data can also be a potential liability to the District if it is lost or improperly disclosed. Accordingly, the Board and District officials are responsible for establishing a District-wide security plan, Disaster Recovery Plan, and policies and procedures for use of mobile storage devices to provide reasonable assurance that the District's valuable IT assets – including computer data, equipment, systems, and media – are properly used and safeguarded against waste, loss, and misuse.

The Board and District officials did not establish adequate policies and procedures to effectively safeguard the District's computer systems and data. Specifically, our audit disclosed that a formal District-wide security plan has not been developed and the Disaster Recovery Plan that is in place is not up-to-date or complete. In addition, there are no policies and procedures for the use of mobile storage devices such as flash drives, and no oversight mechanism for their use. As a result, there is an increased risk that the security measures that are in place may not be effective or followed, the District may not be able to quickly restore operations if a disaster occurred, and the security of the District's computer system and sensitive, confidential data may be compromised.

District-Wide Security Plan

District officials are responsible for developing a formal written District-wide security plan to document the process for evaluating security risks, to identify and prioritize the more dangerous issues, and to document the process for discussing and determining solutions. The plan should establish a framework and continuing process to identify areas of risk, and to develop the policies and procedures to control the risk and monitor the effectiveness of the policies and procedures that were developed.

District officials have determined areas of risk and measures have been put into place to protect the District's assets — for example, the District has implemented a security card system for allowing staff access to certain areas within the building, as well as the building itself, and the District has installed security cameras. However, District

officials have not developed a written security plan to document the processes that are followed or the policies and procedures that were put into place. Without a well-developed, written, District-wide security plan, areas that could be at risk may have been overlooked, and the policies and procedures that were put into place to control risk may not be effective. In addition, employees may not be aware of or may misconstrue the policies and procedures that were developed.

Disaster Recovery Plan

The District's IT system — including equipment, software, and data — is a critical resource that must be protected against loss, damage or misuse. A Disaster Recovery Plan, sometimes referred to as a Business Continuity Plan or Business Process Contingency Plan, describes how an organization should deal with potential disasters. An effective internal control system for IT requires that a formal disaster recovery plan be developed, which includes the precautions to be taken (e.g., the routine backup of software and data) to minimize the effects of a disaster, and the procedures necessary for the District to either maintain or quickly resume mission-critical functions. In addition, the Disaster Recovery Plan must be updated periodically to address changing conditions. Typically, disaster recovery planning involves an analysis of business processes and continuity needs, and may also include a focus on disaster prevention.

The District has developed a Disaster Recovery Plan, which was written by a former Technology Coordinator in 2006. However, the plan has not been updated since its creation. In addition, although the plan identifies preventative measures that the District should follow as part of its normal day-to-day operations to mitigate the effects of a disaster, the plan does not contain written guidelines for staff to follow during or immediately after a disaster. As a result, the District may not be able to continue or restore operations as quickly as possible if a disaster occurs.

Flash Drives

Due to advances in computer technology, the use of mobile storage devices such as flash drives to store and transport information has become very commonplace. These devices can be used almost anywhere, are easily transportable, and can store large amounts of data, documents and other computerized material. Consequently, there are risks associated with their use, such as loss, theft or access by unauthorized individuals. It is therefore necessary for the Board and District officials to develop written policies and procedures to indicate what devices may be used, which individuals are allowed to use them, and how to protect and secure the devices and materials stored on them. The policies and procedures must address the acceptable use of the devices and what to do if problems arise with the devices. In addition, an oversight mechanism must be established to monitor the

types of information that individuals are storing and transporting on these devices.

The Board and District officials have not established policies, procedures, or a mechanism to monitor the information stored and transported on mobile storage devices. As a result, District staff and students use both District issued and personally owned flash drives, that are not secured, on the District's computers and at home. Other than the personal responsibility of the individuals that use the devices, there is no mechanism to safeguard the devices or materials stored on them. If a flash drive was lost or stolen, District officials would have to determine what information was stored on the device and may have been compromised, and whether the device was the primary means of storage for the information. In addition, a malicious employee could use the device to obtain sensitive, confidential, or critical information for fraudulent activities, or to introduce malicious code or malware² into the District's computer system to compromise District data, applications, and operations.

Recommendations

1. District officials should develop a formal, written, District-wide security plan.
2. District officials should develop an updated Disaster Recovery Plan that is comprehensive and provides the direction and guidance necessary to maintain District operations, or restore them as quickly as possible during or following a disaster.
3. The Board and District officials should develop comprehensive written policies and procedures for the use of mobile storage devices such as flash drives.

² Software designed to interfere with a computer's normal functioning

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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



Geneseo Central School District

Timothy C. Hayes
Superintendent

Rosemary Teres
Board President

4050 Avon Road
Geneseo, NY 14454
at David Dwyer Way

Telephone: 585.243.3450
Fax: 585.243.9481

November 6, 2008

████████████████████
Office of the State Comptroller
The Powers Building
16 West Main Street – Suite 522
Rochester, New York 14614-1608

Dear ██████████,

Geneseo Central School is in receipt of the draft Report of Examination of the audit conducted by your office. We also had the opportunity, on October 21, 2008, to meet with ██████████ and ██████████ regarding this draft audit report. I thank you for the opportunity to respond to the audit findings before you issue the final Report of Examination for the Geneseo Central School District. This response letter addresses the findings and recommendations made by your office and will form the basis of our District's corrective action plan.

1. District-Wide Security Plan:

As noted in the report, Geneseo Central School District has established security procedures for determining areas of risk in the District and implementing measures to protect District assets. Protective measures include, but are not limited to, a security card system for staff access and security cameras which allow surveillance throughout our campus. The Geneseo Central Administrative Team, under my direction and supervision, will formulate written plans for staff which detail the protocols utilized to control risks associated with the assets of the District. All plans will be included in the Geneseo Central School District's District-Wide Security Plan. All security plans will be reviewed with appropriate staff members on a yearly basis.

2. Disaster Recovery Plan:

The Geneseo Central School District Technology Committee has begun a review of the District's Disaster Recovery Plan. This plan was originally formulated in 2006. The new Disaster Recovery Plan will include written guidelines for key personnel to follow during and immediately after a disaster that impacts the District's information technology systems. This plan, once rewritten, will be reviewed on an annual basis by the Technology Committee.

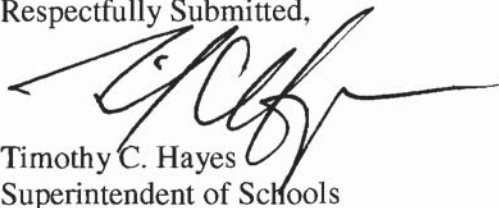
3. Flash Drives:

As part of the Acceptable Use Policies for students and staff of the Geneseo Central School District, written policies and procedures will indicate what devices may be used, which individuals may use them, and how devices and information stored on them will be protected. Acceptable Use Policies will be reviewed by the Geneseo Central School Board of Education during the 2008-2009 school year. Once adopted by the Board of Education, all staff, and students will be required to sign an agreement indicating understanding and acceptance of acceptable use regulations.

The Geneseo Central School District takes seriously the protection of the District's assets and operations. The recommendations in our audit have allowed us to further enhance our security regarding information technology.

The Geneseo Central School District Board of Education was pleased to hear from our auditors that the financial policies and practices in our District were "in tip-top shape." Our District will continue to be attentive in this area in order to protect the assets of our school community.

Respectfully Submitted,



Timothy C. Hayes
Superintendent of Schools

cc: Board of Education
Mrs. Lisa Ryan, Business Administrator

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 District assets. To accomplish this, we performed an initial assessment of the internal controls so that we could design our audit to focus on those areas most at risk. Our initial assessment included evaluations of the following areas: financial oversight, cash receipts and disbursements, purchasing, payroll and personal services, and information technology.

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

After reviewing the information gathered during our initial assessment, we determined where weaknesses existed, and evaluated those weaknesses for the risk of potential fraud, theft and/or professional misconduct. We then decided upon the reported objective and scope by selecting for audit those areas most at risk. We selected information technology for further audit testing.

- We interviewed staff members to determine what internal controls were in place for information technology, including the existence of policies and procedures for security, disaster recovery and the use mobile storage devices, and reviewed the District's Disaster Recovery Plan.
- We interviewed staff members to determine how District staff and students use mobile storage devices such as flash drives, and the existence of oversight mechanisms to monitor what is stored and transported on these devices.

We conducted our performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

APPENDIX C

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller
Public Information Office
110 State Street, 15th Floor
Albany, New York 12236
(518) 474-4015
<http://www.osc.state.ny.us/localgov/>

APPENDIX D
OFFICE OF THE STATE COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY

Steven J. Hancox, Deputy Comptroller
John C. Traylor, Assistant Comptroller

LOCAL REGIONAL OFFICE LISTING

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

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

Eugene A. Camp, 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

BINGHAMTON REGIONAL OFFICE

Patrick Carbone, Chief Examiner
Office of the State Comptroller
State Office Building, Room 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

GLENS FALLS REGIONAL OFFICE

Karl Smoczynski, 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: Clinton, Essex, Franklin, Fulton, Hamilton,
Montgomery, Rensselaer, Saratoga, Warren, Washington
counties

ALBANY REGIONAL OFFICE

Kenneth Madej, Chief Examiner
Office of the State Comptroller
22 Computer Drive West
Albany, New York 12205-1695
(518) 438-0093 Fax (518) 438-0367
Email: Muni-Albany@osc.state.ny.us

Serving: Albany, Columbia, Dutchess, Greene,
Schenectady, Ulster counties

HAUPPAUGE REGIONAL OFFICE

Jeffrey P. Leonard, 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, 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: Orange, Putnam, Rockland, Westchester
counties