

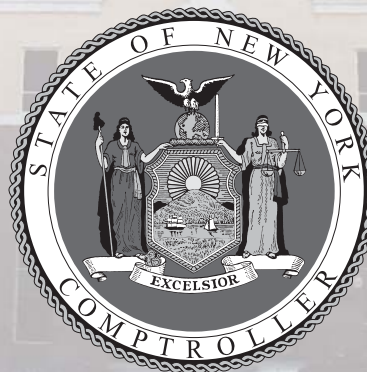


**Mid-Hudson  
Regional Information  
Center  
Internal Controls Over  
Network Security  
Report of Examination**

Period Covered:

February 26, 2006 — November 5, 2007

2008M-120



**Thomas P. DiNapoli**

# Table of Contents

	<b>Page</b>
<b>AUTHORITY LETTER</b>	2
<b>INTRODUCTION</b>	3
Background	3
Objective	4
Scope and Methodology	4
Comments of BOCES Officials and Corrective Action	4
<b>COMPUTER DATA AND ASSETS</b>	5
Administrative Rights	5
Installation of Software	6
Access Controls and Password Management	6
Recommendations	7
<b>APPENDIX A</b> Response From BOCES Officials	9
<b>APPENDIX B</b> OSC Comments on BOCES Officials' Response	14
<b>APPENDIX C</b> Audit Methodology and Standards	15
<b>APPENDIX D</b> How to Obtain Additional Copies of the Report	16
<b>APPENDIX E</b> Local Regional Office Listing	17

# State of New York Office of the State Comptroller

---

---

## **Division of Local Government and School Accountability**

September 2008

Dear Board of Cooperative Educational Services (BOCES) Officials:

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

Following is a report of our audit of the Mid-Hudson Regional Information Center (MHRIC), entitled Internal Controls Over Network Security. 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 BOCES 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 Mid-Hudson Regional Information Center (MHRIC) is a component of the Ulster Board of Cooperative Educational Services (BOCES) which is governed by an 11 member Board of Education (Board) elected by the boards of education of the components districts. The Board is responsible for the general management and control of the BOCES financial and educational affairs. The District Superintendent is the chief executive officer of BOCES and is responsible, along with other administrative staff, for the day-to-day management of BOCES and for regional educational planning and coordination. The Director of Computer Services is responsible for the day-to-day management of the MHRIC.

The MHRIC employs approximately 60 employees and offers technology services to 54 school districts and BOCES in Dutchess, Orange, Sullivan, and Ulster Counties. Services include processing payroll and accounting checks, student schedules, grade reports, and New York State standardized tests. MHRIC has created a computer network (Network) to help carry out its duties. Authorized MHRIC, BOCES and district employees use the Network to access applications, as well as shared files. MHRIC's Operations, Programming, and Technical Services Unit (OPTS) maintains the Network. This includes supporting all servers, hardware configuration, setting up desktop computers, software support, providing network connectivity for all business units, and managing network devices.

Networks are collections of interconnected computer systems and devices that allow individuals to share resources, such as computer programs and information. Because sensitive programs and information are stored on or transmitted along networks, effectively securing networks is essential to protecting computing resources and data from unauthorized access, manipulation, and use. Organizations secure their networks, in part, by installing and configuring network devices that permit authorized network service requests, deny unauthorized requests, and limit the services that are available on the network. Network services consist of protocols for transmitting data between network devices. Insecurely configured network devices and services can make a system vulnerable to internal or external threats. Because networks often include both external and internal access points for electronic information assets, failure to secure these assets increases the risk of unauthorized access to sensitive information and systems, or disruption of service.

**Objective**

The objective of our audit was to evaluate and test controls of the MHRIC's computer network security. Our audit addressed the following related questions:

- Are internal controls relating to external network security appropriately designed and operating effectively?
- Are internal controls over financial and student information servers appropriately designed and operating effectively?

**Scope and Methodology**

We examined the MHRIC's safeguards over computerized data and assets for the period February 26, 2006 to November 5, 2007. Our audit disclosed areas where additional controls and measures must be instituted to help prevent unauthorized access to the Network and servers.

As part of our audit, we identified areas in which the controls needed to be improved, including certain significant weaknesses not discussed in this Report of Examination. Detailed results of our audit tests were provided to MHRIC officials during the conduct of our audit. Because of the sensitive nature of this information, certain specific vulnerabilities are not discussed in this report but have been communicated to MHRIC officials so they could take corrective action. When presented with critical vulnerabilities during our testing, MHRIC officials took prompt remedial 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 are included in Appendix C of this report.

**Comments of District Officials and Corrective Action**

The results of our audit and recommendations have been discussed with BOCES officials and their comments, which appear in Appendix A, have been considered in preparing this report. BOCES officials generally agreed with our recommendations and indicate they plan to initiate corrective action. Our comments concerning the BOCES officials' response can be found in Appendix B.

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.

## Computer Data and Assets

MHRIC officials rely on computerized data to assist them in fulfilling their duties to its component school districts. If the computers on which this data reside fail or if the data is lost or altered, the results could range from inconvenient to catastrophic. Even small disruptions can require extensive effort to evaluate and repair. To this end, installation of unauthorized software should be prevented, and access should be controlled and monitored.

The Board is responsible for adopting policies and developing controls to safeguard computerized data and assets. In addition, the Superintendent and the Director of Computer Services are responsible for ensuring that MHRIC officials and employees adhere to adopted policies and procedures. Although the Board has established some policies, it has not effectively addressed administrative rights, the installation of unauthorized software, and access controls and password security.

### Administrative Rights

Administrative rights allow users to create, delete, and modify files, folders, or settings, including the assignment of users' access rights and the ability to download and install programs. A user with administrative rights (or an unauthorized user who gains access to a system administrator account) can also modify computer-generated log files to cover such actions. Even unintentional changes could cause severe problems. By limiting the number of users having administrative rights – for example, a designated OPTS employee and a backup person – and providing appropriate oversight of their duties, MHRIC officials can significantly reduce the risk of inappropriate changes to the MHRIC's network and data.

According to MHRIC personnel, all end users on the MHRIC network have local administrator rights on their workstations. Allowing end users to have local administrative rights introduces numerous vulnerabilities to the MHRIC network. These vulnerabilities include the installation of unauthorized software and allowing the end user to obtain the password hashes<sup>1</sup> on their local machines.

The indiscriminate assignment of administrative user rights exposes the MHRIC's network and data to an increased risk of loss, corruption, or misuse.

---

<sup>1</sup> A password hash may be thought of as one-way encryption. It is a digital fingerprint of a piece of data; thus it is unique.

## Installation of Software

Prohibiting the installation of unauthorized software by users is a crucial step in preventing potentially harmful software from being installed on the MHRIC's computers. Unauthorized programs could transfer personal or sensitive information to outside networks and/or potentially slow down the Network or cause system crashes.

According to MHRIC officials, the downloading of software onto MHRIC computers is addressed, by extension, in Board Policy 8330 which states that BOCES materials and equipment are to be used only as required by staff in the performance of their assigned duties. MHRIC officials stated that since personal use of the computer is prohibited, the loading of software for personal use is also prohibited. Officials also stated that employees are not prohibited from loading software that is connected with their job duties.

We believe the policy does not sufficiently address the risks associated with installing unauthorized software on MHRIC equipment. For example, the policy does not require users to obtain authorization before software is installed on MHRIC-owned computers and there is no requirement or procedure to monitor the appropriateness of the software downloaded. Also, because users have administrative rights to their computers, there is an additional risk that employees could inadvertently download and install harmful software onto MHRIC-owned computers.

The ability of users to install unauthorized software onto MHRIC-owned computers significantly increases the risk that sensitive or mission-critical data and hardware and software systems may be lost, compromised, or damaged.

## Access Controls and Password Management

Internal controls over access to the IT system provide reasonable assurance that computer resources, which include equipment, data files, application programs, and computer related facilities, are adequately safeguarded. Password management is one aspect of access controls. Passwords are used to mitigate the risk of unauthorized access. System users are generally required to enter user names and passwords to gain access to networks, computers, and applications. To protect computerized data, MHRIC officials should implement or strengthen policies and procedures related to access controls and the use of strong passwords.<sup>2</sup>

To maintain good internal controls, password policies and procedures should require complex passwords that are alphanumeric and contain

---

<sup>2</sup> Strong passwords contain a combination of upper- and lower-case letters, punctuation and at least eight characters.

at least eight characters. The more complex a password is, the better the chances that unauthorized users will be prevented from gaining access. Also, users should be required to change their passwords every 30 to 90 days. To help reduce the risk that passwords can be guessed, the system administrator should limit the number of unsuccessful login attempts to three or four. Password requirements should be built into organizational security policies. Systems administrators should implement automated safeguards to ensure that users on their systems are actually using strong passwords.

We found that MHRIC officials have not adopted comprehensive policies and procedures to address the use of strong passwords, changing passwords and limiting attempts to access the system. The MHRIC does not have a documented password policy in place, and our testing disclosed that the MHRIC needs to make improvements to its password management practices. We communicated specific concerns related to the complexity of passwords in a separate confidential letter to MHRIC officials.

We were able to guess a password of a generic user account on a server in one try. This account had administrative privileges on the server. Using this account, we copied a listing of all user accounts along with their Windows domain password hashes from this server. We then tested the strength of user passwords. We were able to identify all of the domain user account passwords, except for the administrator account and one other user account, in less than five minutes. Knowing these passwords, a person could access other resources on MHRIC's Network.

There were other access control weaknesses that we have communicated in a separate letter, and because of those weaknesses, we were able to log into the system from within the building. We were able to view and could have copied the following: a text file with various school districts' employee information in it, a text file that contained check information that was made out to vendors, and a text file that contained a school district employee's address and banking account number.

If access controls and the password system are not strong and policies and procedures are not established, unauthorized persons could gain access to sensitive systems and data.

## **Recommendations**

1. MHRIC officials should restrict local administrative rights on end-user workstations.
2. MHRIC officials should ensure that a policy explicitly restricting the download and installation of unauthorized software is established and compliance is monitored and enforced. As

part of this policy, MHRIC officials should address computer configuration and authority to install software (as a means to further control the downloading of software).

3. MHRIC officials should ensure that a strong password system exists on all Network devices by adopting policies and procedures that require:
  - The changing of all passwords at regular intervals
  - The creation of strong passwords requiring users to select passwords that are at least eight characters, containing upper- and lower-case letters, and punctuation in order to prevent passwords from being easily guessed or cracked
  - The password history length to be greater than five change cycles
  - Limiting the number of failed login attempts by user account lockouts after a certain number of failed login attempts.
4. The Board should implement the specific recommendations for strengthening Network security that were provided to MHRIC officials during the audit but not included in this report because of their sensitive nature.

## **APPENDIX A**

### **RESPONSE FROM BOCES OFFICIALS**

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

The BOCES response makes reference to an attachment (BOCES Appendix B) that contains confidential network security information. Because of the confidentiality of this information, the attachment is not included in this report.

September 2, 2008

[REDACTED]  
Office of the State Comptroller  
22 Computer Drive West  
Albany, NY 12205

Dear [REDACTED]:

As requested in your letter dated July 30th, 2008, the following is a response to the audit report and a Corrective Action Plan.

First, we appreciate the Comptrollers office bringing these concerns to our attention. We regard our responsibility and accountability to our school districts as an important obligation and it is a priority for this agency. We are responding to your department's observations after careful consideration of the concerns and an in depth review with the Ulster BOCES Board of Education.

Your letter and the exit interview focused on 4 areas of concern (in summary):

- Workstation administrative rights
- Software installation
- Password management
- Network security (confidential) Appendix B

The Mid-Hudson Regional Information Center has reviewed these concerns and provided feedback to the examiners in the exit interview on all of the issues, as re-capped below.

While we agree with most of the findings, we have determined that we may be unable to implement all recommendations as submitted. The basis of this difference is the operational nature of a data center or software limitations that are beyond our control. The following section discusses these areas in detail followed by the Corrective Action Plan that details changes to be implemented.

Due to the sensitive nature of the information contained in this document we request that the sections that address password management and administrative rights be redacted before any public release. Knowledge of how our systems are secured or limitations of the software could be used to subvert the very measures that have been implemented to protect the systems.

See  
Note 1  
Page 14

### Workstation Administrative Rights

Due to the unique functions that the MHRIC performs as a data center, many of our employees require administrative rights to their workstation. These permissions are necessary to perform their jobs.

We operate in a secure building that does not allow casual access by the public or other UB employees. It would be difficult for a person from outside of the organization to gain access to one of our workstations and perpetrate a breach. It should be noted that while it is possible that a workstation could be subverted as described in the Comptroller's report, the risk is overstated.

### Software Installation

We will add the following sentence to Ulster BOCES Board policy 8330. "The loading of software for personal use is prohibited." We also will audit a select number of workstations to insure that they are in compliance with the board policy.

### Password Management

Ulster BOCES does not currently have a board policy that addresses password management. Password administration is managed by each division.

[REDACTED] However we will draft and implement a policy that requires minimum standards for passwords. We intend to implement this policy to the extent that the software packages can accommodate.

### Network and computer security (Confidential)

See attachment and appendix B

In compliance with §35 of the General Municipal Law, Ulster County BOCES herewith submits its Corrective Action Plan in response to the Comptroller's audit letter dated July 30, 2008.

### Corrective Action Plan

The Comptroller's Letter cited the following items as opportunities to strengthen our internal controls and improve operating efficiency.

COMPTROLLER ADVICE	CORRECTIVE ACTION PLAN	POSITION(S) RESPONSIBLE
Limit workstations administrative rights	<ul style="list-style-type: none"> <li>• Remove administrative rights from any workstation where the user does not require these rights to perform their assigned job i.e., clerical staff and classrooms.</li> <li>• Enhance perimeter security by installing an access control system that records building entry.</li> </ul>	MHRIC Director/ Manager of Operations and Programming
Software installation	<ul style="list-style-type: none"> <li>• Add the download of personal software to UB board policy 8330 as a prohibited activity, unless authorized by the MHRIC director for business reasons.</li> <li>• Audit workstations on an annual basis to ensure compliance with policy 8330.</li> </ul>	MHRIC Director/ Manager of Operations and Programming/Ulster BOCES BOE
Define and implement password management policy	<ul style="list-style-type: none"> <li>• Ulster BOCES will develop and implement a password management policy that considers the audit recommendations, recognizing the need to improve security.</li> </ul>	MHRIC Director/ Manager of Operations and Programming/Ulster BOCES BOE
Network Security (confidential)	See Appendix B	MHRIC Director/ Manager of Operations and Programming

This report has been reviewed by the Audit Committee and presented to the Board for its review and approval at the August 27, 2008 meeting. If you have further questions or concerns, please do not hesitate to contact me.

Very truly yours,



Eugene Knudsen  
Director, Mid-Hudson Regional Information Center

Cc. Ulster BOCES Board of Education  
Martin Ruglis, District Superintendent  
Mid-Hudson Joint Management Team  
Asst. Superintendent for Administration

## **APPENDIX B**

### **OSC COMMENTS ON BOCES OFFICIALS' RESPONSE**

#### Note 1

OSC auditors met with BOCES officials on August 4, 2008 to review and discuss the audit findings and recommendations included in the draft report as well as in a separate confidential report letter. We produced the separate report letter to report directly to management those control weaknesses that were determined to be of a sensitive nature. The findings and recommendations contained in the draft report related to administrative rights do not constitute privileged or confidential information. Specific information related to password controls has been removed from this report and has been communicated to MHRIC officials in a separate confidential letter.

## APPENDIX C

### AUDIT METHODOLOGY AND STANDARDS

Our overall goal was to assess the adequacy of the internal controls put in place by officials to safeguard the MHRIC's computer data and assets. To accomplish this, we performed an initial assessment of the internal controls over network security so that we could design our audit to focus on those areas most at risk. During the initial assessment, we interviewed appropriate MHRIC officials, and examined network schematics, flowcharts, and applicable policies and procedures provided by MHRIC officials.

During our audit, we conducted vulnerability assessments of the MHRIC Network's key servers, main firewall, and select desktop computers. These assessments also included discussions with MHRIC staff to gain an understanding of the MHRIC's processes and controls. As part of our audit, we tested security controls by determining whether there is a risk that someone could gain unauthorized access to the Network. In performing these tests, we used various tools and techniques to proactively identify Network vulnerabilities and to determine how these vulnerabilities could be exploited. Our testing included vulnerability scans of specific MHRIC Network servers and applications, and a more in-depth testing of select servers and applications where we deemed it appropriate. All scans had all dangerous (denial of service) tests turned off. Denial of service (DNS) attacks occur when users of a system or the organization as a whole are denied access to resources they would normally expect to have. We also evaluated the MHRIC's core Network firewall by reviewing the implementation of the firewall's software and configurations.

Our audit provides a snapshot of the Network's security for a point in time, and is not intended to provide assurance that our audit tests detected all potential Network vulnerabilities. Further testing is defined throughout this document.

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

## APPENDIX D

### 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 E**  
**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](mailto: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](mailto: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](mailto: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](mailto: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](mailto: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](mailto: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](mailto: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](mailto:Muni-Newburgh@osc.state.ny.us)

Serving: Orange, Putnam, Rockland, Westchester  
counties