

STATE OF NEW YORK  
OFFICE OF THE STATE COMPTROLLER  
110 STATE STREET  
ALBANY, NEW YORK 12236

January 19, 2007

Dr. Frederick A. Wille  
District Superintendent  
Monroe 1 BOCES  
Regional Information Center  
41 O'Connor Road  
Fairport, NY 14450

Dear District Superintendent Wille:

The State Comptroller is statutorily required to audit all school districts, BOCES and charter schools in the State by March 31, 2010. The school district audits, done in conformance with generally accepted government auditing standards, often require us to contact a BOCES Regional Information Center to gather information about a school district's financial management system and information technology infrastructure. Since it would be burdensome for you to have multiple audit teams visit the Monroe 1 BOCES Regional Information Center (RIC) to gather the same or similar information, we assigned one group of examiners to gather the needed information for the audits.

This examination was conducted pursuant to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution and Article 3 of the General Municipal Law. Based upon inquiries made during this examination of the financial software packages and technology infrastructure services provided to component (or cross-contracting) school districts by the RIC, we noted the following conditions that we would like to bring to your attention:

- RIC personnel had unlimited access to the school districts' financial accounts systems. RIC staff had the ability to enter into the financial systems remotely at any of the school districts it services. In addition, RIC staff can make data changes (i.e., errors, corrections, adjustments, etc.) by entering them into the system if requested by district officials. Furthermore, all RIC staff working on the financial system application service were "super users," giving them the ability to access all modules within the financial accounts systems. User accounts should be set up to allow only the minimum access rights the user needs to complete their duties.
- RIC employees are not required to annually review and acknowledge the Acceptable Use Policy. The Acceptable Use Policy is contained in the Employee Handbook that is distributed when an employee is hired, and employees are required to sign for receipt of the handbook.

- RIC officials do not systematically monitor access logs to its server room. The server room is a locked, climate-controlled, fire and water protected room with security cameras to monitor inside and outside the server room. Physical access is granted by electronic access only, and the server room has backup generator power. The electronic access generates a log that contains information about activities that could be a security risk to the system. This may help document evidence of unusual, suspicious, or unexpected activities, indicating that someone has compromised or attempted to compromise the system.
- RIC officials have not developed a written disaster recovery plan. A Disaster Recovery Plan (DRP) - sometimes referred to as a Business Continuity Plan (BCP) or Business Process Contingency Plan (BPCP) - describes how an organization is to deal with potential disasters. A plan consists of the precautions taken so that the effects of a disaster will be minimized, and the organization will be able to either maintain or quickly resume mission-critical functions. Typically, disaster recovery planning involves an analysis of business processes and continuity needs; it may also include a significant focus on disaster prevention.
- The RIC does not have written contracts with the school districts that it supplies technology assets to. A written contract would spell out the rights and responsibilities of each party in regards to ownership, maintenance and disposal of technology assets.

As part of our examination, we also identified a potentially sensitive control weakness about the financial management system and information technology infrastructure maintained by the RIC. Publicly disclosing information about this weakness might create additional risks, so for security reasons we have removed the finding from our final report and redacted all references to it in the attached RIC response letter.

We hope that this information will help you identify areas where you can improve your operations. In order to keep our database of information current, we will be contacting appropriate RIC officials within 90 days to update our information. Furthermore, we will likely continue to contact RIC officials annually to keep our information current.

To clarify, our inquiries on the financial management and infrastructure services that you provide to component (or cross-contracting) school districts is not part of the statutorily required audit of each BOCES. We will contact you again when we plan to start an audit of the BOCES.

The results of our examination were discussed with RIC and BOCES officials and their comments, which appear in Appendix A, have been considered in preparing this report. Officials generally agreed with the conditions cited in our final report and indicated they planned to initiate corrective action. OSC comments to the official response are included in Appendix B.

The Monroe 1 BOCES Board has the responsibility to initiate corrective action. Pursuant to Section 35 of the General Municipal Law, Section 2116-a (3)(c) of the Education Law and Section 170.12 of the Regulations of the Commissioner of Education, the Board must approve a corrective action plan that addresses the conditions cited in this report, forward the plan to our office within 90 days, forward a copy of the plan to the Commissioner of Education and make

the plan available for public review in the Board Clerk's office. For guidance in preparing the plan of action, the Board should refer to applicable sections in the publication issued by the Office of the State Comptroller entitled *Local Government Management Guide*.

If you have any questions, please contact our Rochester regional office at (585) 454-2460.

Sincerely,

A handwritten signature in black ink, appearing to read "Steven J. Hancox". The signature is fluid and cursive, with a prominent initial "S" and a long, sweeping underline.

Steven J. Hancox  
Assistant Comptroller  
Local Government Services  
and Economic Development

## **APPENDIX A**

### **RESPONSE FROM BOCES OFFICIALS**

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



**BOARD OF COOPERATIVE EDUCATIONAL SERVICES**  
First Supervisory District of Monroe County

Dr. Frederick A. Wille, *District Superintendent*  
Monroe #1 BOCES  
41 O'Connor Road  
Fairport, New York 14450  
(585) 377-4660  
www.monroe.edu

To: Office of the Comptroller  
From: Dr. Fred Wille *[Signature]*  
Re: Plan of Action  
Date: December 18, 2006

On September 15, 2006, John Poland, Bonnie Garner and I met with two representatives from the comptroller's office. The purpose of this meeting was to review information that was collected during the comptroller's visit to the Monroe #1 BOCES Regional Information Center on February 14, 2006.

There were six conditions that we would like to address and respond to are listed below:

1. **Condition:** RIC personnel had unlimited access to the school districts' financial account systems. RIC staff can enter both the [REDACTED] and [REDACTED] systems remotely at any of the school districts it services. With this type of access the staff can make data changes and access all modules within the accounts system.

**Response:** Monroe #1 RIC is developing a policy that requires a monthly audit log to be generated by the software that is sent to the district and reviewed by the RIC. This audit log lists any access to the financial system by any financial support person either Monroe #1 RIC employee or district personnel at any time. The audit log will be retained by the RIC Director. In addition, all user accounts are now set to allow only the minimum access rights the user needs to complete their duties.

2. **Condition:** RIC employees are not required to annually review and acknowledge the Acceptable Use Policy. The policy is signed when an employee is hired.

**Response:** RIC employees are now asked to sign an AUP at the start of each school year. At the October 3, 2006 staff meeting, all RIC personnel will be required to review and sign the Acceptable Use Policy. This will be a yearly requirement for all RIC personnel.

3. **Condition:** RIC officials do not systematically monitor access logs to its server room. Physical access is granted by electronic access only which generates a log. The server room is a locked, climate controlled, fire and water protected room with security cameras to monitor inside and outside the server room. The electronic access generates a log that contains information about activities that could be a security risk to the system.

**Response:** The server room with the electronic access log can assist in identifying any evidence of unusual, suspicious, or unexpected activities indicating that someone has compromised or attempted to compromise the system. Access to the server room is approved by the RIC Director. This log will be monitored by RIC Director on a monthly basis to ensure a secure environment.

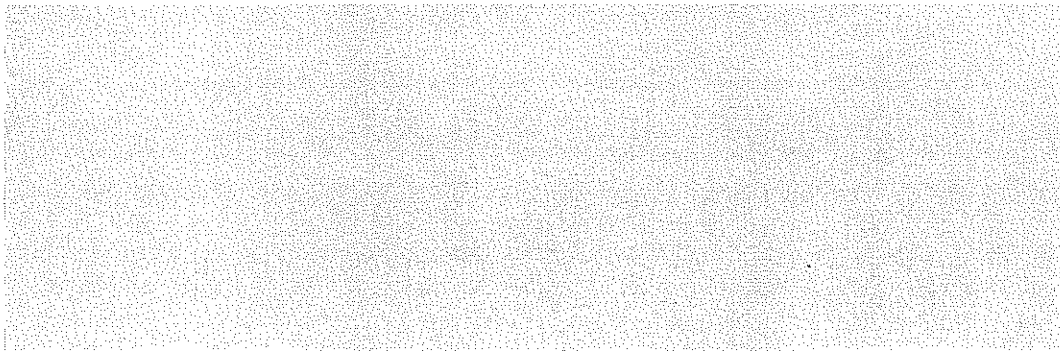
4. **Condition:** RIC officials have not developed a written disaster recovery plan. A plan consists of the precautions taken so that the effects of a disaster will be minimized, and the organization will be able to either maintain or quickly resume business processes and continuity needs.

**Response:** Monroe #1 RIC does need to have an updated disaster recover plan. At the present time, RIC officials are working with an independent consultant to develop a comprehensive business continuity plan. The targeted date for completion is March 30, 2007. We are working with school districts and BOCES to guarantee that essential operations will be able to continue in the event of an emergency.

5. **Condition:** The RIC does not have written contracts with the school districts that it supplies technology assets to.

**Response:** The Monroe #1 RIC is in the process or developing a written contract for all technology assets. This contract will spell out the rights and responsibilities for each party (school district and BOCES) in regards to ownership, maintenance and disposal of technology assets. This contract will be signed by districts annually.

6.



See  
Note 1  
Page 7

## **APPENDIX B**

### **OSC COMMENTS TO BOCES RESPONSE**

#### Note 1

Officials provided us additional information after the completion of our fieldwork. As a result, we removed one finding from our final report. We redacted the officials' response on this matter because it contained confidential information that may raise security issues.