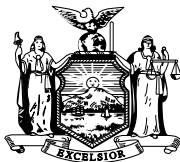


THOMAS P. DiNAPOLI
STATE COMPTROLLER



110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

April 20, 2007

Ms. Jacklin G. Starks
District Superintendent
Madison-Oneida BOCES
Mohawk Regional Information Center
4937 Spring Brook Rd.
Verona, NY 13478

Report Number: 2006M-160

Dear District Superintendent Starks:

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 Madison-Oneida BOCES Mohawk 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:

- Back up tapes are maintained on site Monday through Friday; on Friday, they are moved next door to the RIC administration building. After one week, they are moved off-site for a week, and then returned and reused. This system leaves two weeks of backups at risk of loss. The failure to maintain daily backup off-site could lead to the loss of data.
- The RIC has not tested the performance of its 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. Without testing, it is possible that certain aspects of the plan will not function as expected, leaving the BOCES business processes and continuity at risk.

- At least four RIC personnel had the ability to access districts' financial accounting systems and related servers using a common account with "super user rights" to modify user accounts and change passwords. An audit trail detailing these individuals' activity was not in operation. Such a mitigating control, if operating effectively, could reduce the risk associated with providing RIC officials with unlimited access to district financial systems.
- RIC personnel print checks for several school districts using signature disks stored at the RIC. Signature disks should remain under the control of the school district treasurer at all times.

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 report and indicated they planned to initiate corrective action. OSC comments on the BOCES response are included in Appendix B.

The Madison-Oneida 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 should prepare a plan of action that addresses the recommendations in this report letter and forward the plan to our office within 90 days. For guidance in preparing the plan of action, the Board may refer to applicable sections in the publication issued by the Office of the State Comptroller entitled *Local Government Management Guide*. We encourage the Board to make this plan available for public review in the Clerk of the Board's office.

If you have any questions, please contact our Syracuse regional office (315) 428-4192.

Sincerely,

Steven J. Hancox
Assistant Comptroller

APPENDIX A

RESPONSE FROM BOCES OFFICIALS

The response from BOCES and RIC officials can be found on the following pages.

MADISON-ONEIDA
BOARD OF COOPERATIVE EDUCATIONAL SERVICES

"Enabling Learners to Excel"

DR. PAUL M. SEVERSKY
Deputy Superintendent
pseversky@mbooces.org

4937 Spring Road, PO. Box 168
Verona, New York 13478-0168
Phone 315-361-5520, Fax 315-361-5517

April 4, 2007

[REDACTED]
[REDACTED] of Local Government Services and Economic Development
Office of the NY State Comptroller
110 State Street
Albany, NY 12236

Dear [REDACTED]

Please find our response to Report Number: 2006M-160 Draft Mohawk Regional Information Center IT examination below:

➤ Preliminary Draft Finding 1:

Back up tapes are maintained on-site Monday through Friday; on Friday, they are moved next door to the RIC administration building. After one week, they are moved off-site for a week, and then returned and reused. This system leaves two weeks of backups at risk of loss. The failure to maintain daily backup off-site could lead to the loss of data.

Response and Actions:

- In order to maintain efficient processing and instant restoration processes at the RIC it is necessary to have daily backups available on-site. To respond to off-site backup concerns, we will do the following:
 1. Keep the current rotation schedule for the tape backups
 2. Implement a secure File Transfer Protocol (FTP) server at our off-site Disaster Recovery location
 3. Put backup files daily to the FTP server at the Disaster Recovery location

➤ Preliminary Draft Finding 2:

The RIC has not tested the performance of its 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. Without testing, it is possible that certain aspects of the plan will not function as expected, leaving BOCES business processes and continuity at risk.

Response and Actions:

- The Disaster Recovery Plan of the MORIC outlines current practices and procedures, recovery operations, and serves as a roadmap to lead the recovery team from the incident, through a decision making process, to implementation of restored services. The following scenarios will be implemented to test the scope of this plan:

1. Finalize appropriate climate control, wiring, and server security at the [REDACTED] (alternative processing site) with the Building and Grounds Supervisor and the Deputy Superintendent.
2. Add Disaster Recovery Plan testing to the Management Plans for the Programming & Systems Team for 2007-2008.
3. Modify Section 2.1 of the Disaster Recovery Plan on Data Backup and Restoration to include the use of the FTP server for additional daily backup functionality (as defined in Finding 1.)
4. Section 3.1 of the Recovery Process is currently in effect.
 - Copies of Security Policy Handbooks and Disaster Recovery Plans are in separate safes with the Director of the RIC, Sr. Systems Analyst, Team Leaders, and the Manager of Operations
 - The Call Tree is in effect and has been tested
5. Section 3.2 of the Disaster Recovery Plan for Critical Services and Recovery Priorities is in process.
 - Secure and set up a location for equipment.
 - Methods to re-establish communication with customer and staff have been thoroughly defined within the plan and will be tested by team listed in #2.
 - Methods to re-establish Financial Services have been thoroughly defined within the plan and will be tested by the team listed in #2.
 - Additional alternative site processing, as defined in Section 3.2.4 of the Disaster Recovery Plan, will be tested with the North East Regional Information Center and Capital Computer Associates.

➤ Preliminary Draft Finding 3:

At least four RIC personnel had the ability to access districts' financial accounting systems and related services using a common account with "super user rights" to modify user accounts and change passwords. An audit trail detailing these individuals' activity was not in operation. Such a mitigating control, if operating effectively, could reduce the risk associated with providing RIC officials with unlimited access to district financial systems.

Response and Actions:

- All RIC financial coordination staff supporting MORIC districts using [REDACTED] [REDACTED] or [REDACTED] have been assigned individual user id's and passwords for all RIC personnel. Both [REDACTED] and [REDACTED] produce audit trails and related reports that show activity by individual users including all MORIC staff and these audit trails are operational.

See Note 1 Page 7

➤ Preliminary Draft Finding 4:

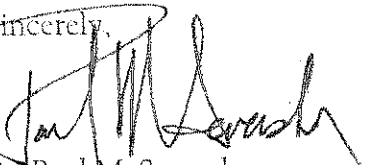
RIC personnel print checks for several school districts using signature disks stored at the RIC. Signature disks should remain under the control of the school district treasurer at all times.

Response and Actions:

- There are checks and balances currently in place for the signature print process. For example, [REDACTED] only allows MORIC staff to print checks when the payroll and accounting schedules are closed electronically by authorized personnel from each district.
- MORIC staff will work with the [REDACTED] and [REDACTED] vendors to develop a new signature print process from a secure server directory located at the RIC or the school district. With this scenario, signatures would reside in an encrypted limited access directory. Accompanying this scenario would be a signed release from the school district Superintendent authorizing the RIC to house the encrypted signature for use on payroll and accounts payable checks only.

Based on this response to your Draft Report Number: 2006M-160, I would appreciate your consideration to modify these findings from the draft report before the final report is filed by your office. Thank you for your consideration.

Sincerely,



Dr. Paul M. Seversky
Deputy Superintendent
Madison-Oneida BOCES

- c Jacklin Starks, District Superintendent
Joan Sotherden, Director
Lisa Decker, Director of Finance
Marlene Derminio, N&T Team Leader
Amanda Palmer, Financial Team Leader

APPENDIX B

OSC COMMENTS ON THE BOCES RESPONSE

Note 1

While assigning individual user IDs and passwords and having an operational audit trail enhance internal controls, the BOCES did not indicate whether district officials are either provided the audit logs or made aware that they are available. Furthermore, there is no indication that the audit logs are periodically reviewed to ascertain whether improper or unauthorized activity is occurring.