MOUNT PLEASANT AREA SCHOOL DISTRICT

WESTMORELAND COUNTY, PENNSYLVANIA

PERFORMANCE AUDIT REPORT

JUNE 2011

The Honorable Tom Corbett
Governor
Commonwealth of Pennsylvania
Harrisburg, Pennsylvania 17120

Mr. Robert Gumbita, Board President
Mount Pleasant Area School District
271 State Street
Mount Pleasant, Pennsylvania 15666

Dear Governor Corbett and Mr. Gumbita:

We conducted a performance audit of the Mount Pleasant Area School District (MPASD) to determine its compliance with applicable state laws, regulations, contracts, grant requirements and administrative procedures. Our audit covered the period April 18, 2008 through November 22, 2010, except as otherwise indicated in the report. Additionally, compliance specific to state subsidy and reimbursements was determined for the school years ended June 30, 2008 and June 30, 2007. Our audit was conducted pursuant to 72 P.S. § 403 and in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States.

Our audit found that the MPASD complied, in all significant respects, with applicable state laws, regulations, contracts, grant requirements, and administrative procedures. However, we identified one matter unrelated to compliance that is reported as an observation. A summary of these results is presented in the Executive Summary section of the audit report.

Our audit observation and recommendations have been discussed with MPASD's management and their responses are included in the audit report. We believe the implementation of our recommendations will improve MPASD's operations and facilitate compliance with legal and administrative requirements. We appreciate the MPASD's cooperation during the conduct of the audit and their willingness to implement our recommendations.

Sincerely,

/s/
JACK WAGNER
Auditor General

June 21, 2011

MOUNT PLEASANT AREA SCHOOL DISTRICT Board Members

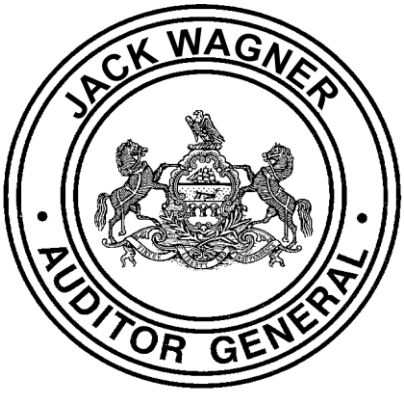
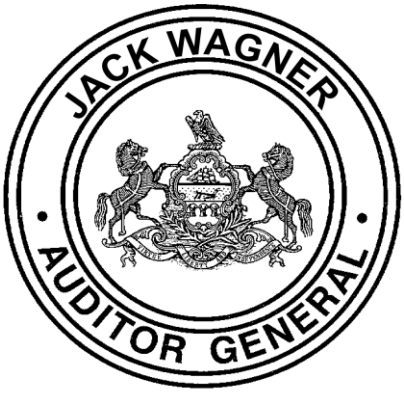

JACK WAGNER
AUDITOR GENERAL

Table of Contents


JACK WAGNER
AUDITOR GENERAL

Executive Summary

Audit Work

The Pennsylvania Department of the Auditor General conducted a performance audit of the Mount Pleasant Area School District (MPASD). Our audit sought to answer certain questions regarding the District's compliance with applicable state laws, regulations, contracts, grant requirements, and administrative procedures; and to determine the status of corrective action taken by the MPASD in response to our prior audit recommendations.

Our audit scope covered the period April 18, 2008 through November 22, 2010, except as otherwise indicated in the audit scope, objectives, and methodology section of the report. Compliance specific to state subsidy and reimbursements was determined for school years 2007-08 and 2006-07.

District Background

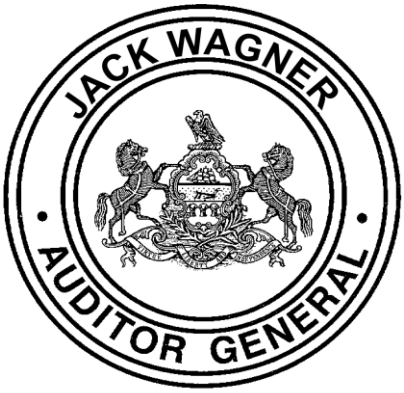
The MPASD encompasses approximately 105 square miles. According to 2000 federal census data, it serves a resident population of 18,488. According to District officials, in school year 2007-08, the MPASD provided basic educational services to 2,283 pupils through the employment of 169 teachers, 45 full-time and part-time support personnel, and 11 administrators. Lastly, the MPASD received more than $13.1 million in state funding in school year 2007-08.

Audit Conclusion and Results

Our audit found that the MPASD complied, in all significant respects, with applicable state laws, regulations, contracts, grant requirements, and administrative procedures; however, as noted below, we identified one matter unrelated to compliance that is reported as an observation.

Observation: Unmonitored Vendor System Access and Logical Access Control Weaknesses. We determined that a risk exists that unauthorized changes to the MPASD's data could occur and not be detected because the MPASD was unable to provide supporting evidence that it is adequately monitoring all vendor activity in its system. This observation was also made in our previous audit report (see page 6).

Status of Prior Audit Findings and Observations. With regard to the status of our prior audit recommendations to the MPASD, we found the MPASD had not taken appropriate corrective action in implementing our recommendations pertaining to unmonitored vendor system access and logical access control weaknesses (see page 11).


JACK WAGNER
AUDITOR GENERAL

Audit Scope, Objectives, and Methodology

Scope

What is a school performance audit?

School performance audits allow the Department of the Auditor General to determine whether state funds, including school subsidies, are being used according to the purposes and guidelines that govern the use of those funds. Additionally, our audits examine the appropriateness of certain administrative and operational practices at each Local Education Agency (LEA). The results of these audits are shared with LEA management, the Governor, the PA Department of Education, and other concerned entities.

Our audit, conducted under authority of 72 P.S. § 403, is not a substitute for the local annual audit required by the Public School Code of 1949, as amended. We conducted our audit in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States.

Our audit covered the period April 18, 2008 through November 22, 2010, except for the verification of professional employee certification which was performed for the period July 1, 2010 through September 30, 2010.

Regarding state subsidy and reimbursements, our audit covered school years 2007-08 and 2006-07.

While all districts have the same school years, some have different fiscal years. Therefore, for the purposes of our audit work and to be consistent with Department of Education (DE) reporting guidelines, we use the term school year rather than fiscal year throughout this report. A school year covers the period July 1 to June 30.

Objectives

What is the difference between a finding and an observation?

Our performance audits may contain findings and/or observations related to our audit objectives. Findings describe noncompliance with a law, regulation, contract, grant requirement, or administrative procedure. Observations are reported when we believe corrective action should be taken to remedy a potential problem not rising to the level of noncompliance with specific criteria.

Performance audits draw conclusions based on an evaluation of sufficient, appropriate evidence. Evidence is measured against criteria, such as, laws, regulations, and defined business practices. Our audit focused on assessing the MPASD's compliance with applicable state laws, regulations, contracts, grant requirements and administrative procedures. However, as we conducted our audit procedures, we sought to determine answers to the following questions, which serve as our audit objectives:

- ✓ Were professional employees certified for the positions they held?
- ✓ Is the District's pupil transportation department, including any contracted vendors, in compliance with applicable state laws and procedures?
- ✓ Are there any declining fund balances which may impose risk to the fiscal viability of the District?

- ✓ Did the District pursue a contract buyout with an administrator and if so, what was the total cost of the buy-out, reasons for the termination/settlement, and do the current employment contract(s) contain adequate termination provisions?

- ✓ Were there any other areas of concern reported by local auditors, citizens, or other interested parties which warrant further attention during our audit?

- ✓ Is the District taking appropriate steps to ensure school safety?

- ✓ Did the District use an outside vendor to maintain its membership data and if so, are there internal controls in place related to vendor access?

- ✓ Did the District take appropriate corrective action to address recommendations made in our prior audits?

Methodology

Government Auditing Standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings, observations 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.

What are internal controls?

Internal controls are processes designed by management to provide reasonable assurance of achieving objectives in areas such as:

- Effectiveness and efficiency of operations;
- Relevance and reliability of operational and financial information;
- Compliance with applicable laws, regulations, contracts, grant requirements and administrative procedures.

MPASD management is responsible for establishing and maintaining effective internal controls to provide reasonable assurance that the District is in compliance with applicable laws, regulations, contracts, grant requirements, and administrative procedures. Within the context of our audit objectives, we obtained an understanding of internal controls and assessed whether those controls were properly designed and implemented.

Any significant deficiencies found during the audit are included in this report.

In order to properly plan our audit and to guide us in possible audit areas, we performed analytical procedures in the areas of state subsidies/reimbursement, pupil membership, pupil transportation, and comparative financial information.

Our audit examined the following:

- Records pertaining to bus driver qualifications, professional employee certification, and financial stability.
- Items such as Board meeting minutes.

Additionally, we interviewed selected administrators and support personnel associated with MPASD operations.

Lastly, to determine the status of our audit recommendations made in a prior audit report released on April 1, 2009, we reviewed the MPASD's response to DE dated May 11, 2009. We then performed additional audit procedures targeting the previously reported matters.

Findings and Observations

Observation

Unmonitored Vendor System Access and Logical Access Control Weaknesses

What is logical access control?

"Logical access" is the ability to access computers and data via remote outside connections.

"Logical access control" refers to internal control procedures used for identification, authorization, and authentication to access the computer systems.

The Mount Pleasant Area School District uses software purchased from an outside vendor for its critical student accounting applications (membership and attendance). The software vendor has remote access into the District's network servers.

Based on our audit procedures, we determined that a risk exists that unauthorized changes to the District's data could occur and not be detected because the District was unable to provide supporting evidence that it is adequately monitoring all vendor activity in its system. However, since the District has adequate manual compensating controls in place to verify the integrity of the membership and attendance information in its database, that risk is mitigated.

Reliance on manual compensating controls becomes increasingly problematic if the District would ever experience personnel and/or procedure changes that could reduce the effectiveness of the manual controls. Unmonitored vendor system access and logical access control weaknesses could lead to unauthorized changes to the District's membership information and result in the District not receiving the funds to which it was entitled from the state.

During our review, we again found the following weaknesses over vendor access to the District's system:

1. The District does not have evidence that it is generating or reviewing monitoring reports of user access and activity on the system (including vendor and District employees). There is no evidence that the District is performing procedures to determine which data the vendor may have altered or which vendor employees accessed the system.

2. The District does not maintain proper documentation to evidence that terminated employees were removed from the system in a timely manner.

3. The District was unable to provide evidence that it requires written authorization for adding, deleting, or changing a userID.

4. The District does not require written authorization prior to the updating/upgrading of key applications or changing user data.

5. The District does not store data back-ups in a secure, off-site location.

6. The District does not have current information technology (IT) policies and procedures for controlling the activities of vendors/consultants, nor does it require the vendor to sign the District's Acceptable Use Policy.

7. The District's Acceptable Use Policy does not include provisions for privacy (e.g., monitoring of electronic mail, access to files), accountability (responsibilities of users, auditing, incident handling), authentication (password security and syntax requirements), and violations/incidents (what is to be reported and to whom). Further, the employees are not required to sign the policy.

8. The District does not have current policies or procedures in place to analyze the impact of proposed program changes in relation to other business-critical functions.

9. The District has certain weaknesses in logical access controls. We noted that the District's system parameters settings do not require all users, including the vendor, to change passwords every 30 days; to maintain a password history (i.e., approximately ten passwords; to lock out users after three unsuccessful attempts; and to log off the system after a period of inactivity (i.e., 60 minutes maximum).

10. The District has certain weaknesses in environmental controls in the room that contains the server housing all of the District's data. We noted that the specific location does not have fire detection equipment.

Recommendations

The *Mount Pleasant Area School District* should:

1. Generate monitoring reports (including firewall logs) of vendor and employee access and activity on the District's system. Monitoring reports should include the date, time, and reason for access, changes made and who made the changes. The District should review these reports to determine that the access was appropriate and that data was not improperly altered. The District should also ensure it is maintaining evidence to support this monitoring and review.

2. Maintain documentation to evidence that terminated employees are properly removed from the system in a timely manner.

3. Develop policies and procedures to require written authorization when adding, deleting, or changing a userID.

4. Allow upgrades/updates to the District's system only after receipt of written authorization from appropriate District officials.

5. Store back-up tapes in a secure, off-site location.

6. Establish separate IT policies and procedures for controlling the activities of vendors/consultants and have the vendor sign this policy, or require the vendor to sign the District's Acceptable Use Policy.

7. Include provisions in the District's Acceptable Use Policy for privacy (e.g., monitoring of electronic mail, access to files), accountability (responsibilities of users, auditing, incident handling), authentication (password security and syntax requirements), and violations/incidents (what is to be reported and to whom). Further, all employees should be required to sign this policy.

8. Establish policies and procedures to analyze the impact of proposed program changes in relation to other business critical functions.

9. Implement a security policy and system parameter settings to require all users, including the vendor, to

change passwords on a regular basis (i.e., every 30 days). Also, the District should maintain a password history that will prevent the use of a repetitive password (i.e., last ten passwords), lock out users after three unsuccessful attempts, and log users off the system after a period of inactivity (i.e., 60 minutes maximum).

10. Consider implementing additional environmental controls around the network server sufficient to satisfy the requirements of the manufacturer of the server and to ensure warranty coverage. Specifically, the District should install fire alarms in the computer room.

Management Response

Management stated the following:

While the findings are correct and accurate, we respectfully disagree with the premise of the findings. The concern seems to center around the ability of our student software and financial software vendor . . . having the ability to remotely access the software associated with these programs, and potentially access the associated data. While we agree that the vendor does have access to the software packages, and the information contained therein, that access is monitored in several ways. The vendor must access by use of individual usernames and passwords, thereby identifying who is accessing the programs, and additionally an automatic record of all accesses is created, so that at no time can anyone access the software, or data, without identifying who they are, and the purpose of their logging in.

Additionally, the vendor agreement . . . specifically outlines several additional steps to protect the District's data. Within the Software Maintenance Agreement, [the vendor] in item (6) "agrees that its access to Client's computer system shall be limited to resolution of problems reported by Client and related services under this Agreement." Additionally in item (12) "It is understood that [the vendor] may need to access Client's data files in the routine performance of [its] duties under this Agreement. In such event, [the vendor] shall treat all Client data, network access and login information in a confidential manner. Unless specifically required by law, [the vendor] shall not release Client data to any third party without the prior written consent of Client. In instances where Client requests [the vendor] to submit data on Client's behalf,

Client shall provide [the vendor] with a written request in advance of such submission(s)."

While the concern with access to student data and financial data is a valuable concern, the District feels confident that its data is secure, maintained on its own servers, with limited access to the vendor in order that they can maintain software, provide updates, and technical support as needed. The need for any additional steps would only create burdensome barriers to the assistance of our employees when help and assistance is needed.

Auditor Conclusion

While management states that vendor access can be monitored, we were provided no evidence that such monitoring is occurring, as we recommended in our prior audit.

We again recommend that the District implement all of our recommendations, which are based on guidelines published by various sources, to protect the integrity of the District data.

Status of Prior Audit Findings and Observations

Our prior audit of the Mount Pleasant Area School District (MPASD) for the school years 2005-06 and 2004-05 resulted in one reported observation. The observation pertained to the risk that unauthorized changes to the District's data could occur and not be detected. As part of our current audit, we determined the status of corrective action taken by the District to implement our prior recommendations. We analyzed the MPASD Board's written response provided to the Department of Education, performed audit procedures, and questioned District personnel regarding the prior observation. As shown below, we found that the MPASD did not implement recommendations concerning the risk that unauthorized changes could occur to the District's data.

School Years 2005-06 and 2004-05 Auditor General Performance Audit Report

Observation: **Unmonitored Vendor System Access and Logical Access Control Weaknesses**

Observation Summary: The MPASD uses software purchased from an outside vendor for its critical student accounting applications (membership and attendance). The software vendor has remote access into the District's network servers.

Based on our audit procedures, we determined that a risk existed that unauthorized changes to the District's data could occur and not be detected because the District was unable to provide supporting evidence that it was adequately monitoring all vendor activity in its system.

Recommendations: Our audit observation recommended that the MPASD:

1. Generate monitoring reports (including firewall logs) of vendor and employee access and activity on the District's system. Monitoring reports should include the date, time, and reason for access, changes made and who made the changes. The District should review these reports to determine that the access was appropriate and that data was not improperly altered. The District should also ensure it is maintaining evidence to support this monitoring and review.

2. Maintain documentation to evidence that terminated employees are properly removed from the system in a timely manner.

3. Develop policies and procedures to require written authorization when adding, deleting, or changing a userID.

4. Allow upgrades/updates to the District's system only after receipt of written authorization from appropriate District officials.

5. Store back-up tapes in a secure, off-site location.

6. Establish separate information technology policies and procedures for controlling the activities of vendors/consultants and have the vendor sign this policy, or require the vendor to sign the District's Acceptable Use Policy.

7. Include provisions in the District's Acceptable Use Policy for privacy (e.g., monitoring of electronic mail, access to files), accountability (responsibilities of users, auditing, incident handling), authentication (password security and syntax requirements), and violations/incidents (what is to be reported and to whom). Further, all employees should be required to sign this policy.

8. Establish policies and procedures to analyze the impact of proposed program changes in relation to other business critical functions.

9. Implement a security policy and system parameter settings to require all users, including the vendor, to change passwords on a regular basis (i.e., every 30 days). Also, the District should maintain a password history that will prevent the use of a repetitive password (i.e., last ten passwords), lock out users after three unsuccessful attempts, and log users off the system after a period of inactivity (i.e., 60 minutes maximum).

10. Consider implementing additional environmental controls around the network server sufficient to satisfy the requirements of the manufacturer of the server and to ensure warranty coverage. Specifically, the District should install fire alarms in the computer room.

Current Status: Based on the results of our current audit, we concluded that the MPASD did not take corrective action to address this observation. It is therefore being carried forward to the current audit (see the observation on page 6).

Distribution List

This report was initially distributed to the superintendent of the school district, the board members, our website address at www.auditorgen.state.pa.us, and the following:

The Honorable Tom Corbett
Governor
Commonwealth of Pennsylvania
Harrisburg, PA 17120

The Honorable Ronald J. Tomalis
Secretary of Education
1010 Harristown Building #2
333 Market Street
Harrisburg, PA 17126

The Honorable Robert M. McCord
State Treasurer
Room 129 - Finance Building
Harrisburg, PA 17120

Ms. Barbara Nelson
Director, Bureau of Budget and
Fiscal Management
Department of Education
4th Floor, 333 Market Street
Harrisburg, PA 17126

Dr. David Wazeter
Research Manager
Pennsylvania State Education Association
400 North Third Street - Box 1724
Harrisburg, PA 17105

Dr. David Davare
Director of Research Services
Pennsylvania School Boards Association
P.O. Box 2042
Mechanicsburg, PA 17055

This report is a matter of public record. Copies of this report may be obtained from the Pennsylvania Department of the Auditor General, Office of Communications, 318 Finance Building, Harrisburg, PA 17120. If you have any questions regarding this report or any other matter, you may contact the Department of the Auditor General by accessing our website at www.auditorgen.state.pa.us.