PINE GROVE AREA SCHOOL DISTRICT

SCHUYLKILL COUNTY, PENNSYLVANIA

PERFORMANCE AUDIT REPORT

JANUARY 2010

The Honorable Edward G. Rendell
Governor
Commonwealth of Pennsylvania
Harrisburg, Pennsylvania 17120

Ms. Rosemary Kramer, Board President
Pine Grove Area School District
103 School Street
Pine Grove, Pennsylvania 17963

Dear Governor Rendell and Ms. Kramer:

We conducted a performance audit of the Pine Grove Area School District (PGASD) to
determine its compliance with applicable state laws, regulations, contracts, grant requirements,
and administrative procedures. Our audit covered the period June 26, 2007 through
October 15, 2009, 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 PGASD 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 PGASD's management and their responses are included in the audit report. We believe the implementation of our recommendations will improve PGASD's operations and facilitate compliance with legal and administrative requirements. We appreciate the PGASD's cooperation during the conduct of the audit and their willingness to implement our recommendations.

Sincerely,

/s/
JACK WAGNER
January 29, 2010   Auditor General

cc: **PINE GROVE AREA SCHOOL DISTRICT** Board Members

Table of Contents

Executive Summary

Audit Work

The Pennsylvania Department of the Auditor General conducted a performance audit of the Pine Grove Area School District (PGASD). 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 PGASD in response to our prior audit recommendations.

Our audit scope covered the period June 26, 2007 through October 15, 2009, 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 PGASD encompasses approximately 109 square miles. According to 2000 federal census data, it serves a resident population of 11,284. According to District officials, in school year 2007-08 the PGASD provided basic educational services to 1,729 pupils through the employment of 141 teachers, 67 full-time and part-time support personnel, and 19 administrators. Lastly, the PGASD received more than $9.6 million in state funding in school year 2007-08.

Audit Conclusion and Results

Our audit found that the PGASD 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 IU System Access and Logical Access Control Weaknesses. We noted that PGASD personnel should improve controls over remote access to its computers. In particular, controls should be strengthened over outside vendor access to the student accounting applications (see page 6).

Status of Prior Audit Findings and Observations. With regard to the status of our prior audit recommendations to the PGASD from an audit we conducted of the 2005-06 and 2004-05 school years, we found the PGASD had taken appropriate corrective action in implementing our recommendations pertaining to our observation regarding the PGASD's Memorandum of Understanding not being updated in a timely matter (see page 13).

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 June 26, 2007 through October 15, 2009.

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 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

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 PGASD'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?

✓ Did the District follow applicable laws and procedures in areas dealing with pupil membership and ensure that adequate provisions were taken to protect the data?

✓ 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?

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.

✓ 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 take appropriate corrective action to address recommendations made in our prior audits?

Methodology

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.

Government Auditing Standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our observation and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our observation and conclusions based on our audit objectives.

PGASD's 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 and pupil transportation.

Our audit examined the following:

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

Additionally, we interviewed selected administrators and support personnel associated with PGASD's operations.

Lastly, to determine the status of our audit recommendations made in a prior audit report released on October 22, 2007, we then performed additional audit procedures targeting the previously reported matters.

Findings and Observations

Observation ———————————▶

Unmonitored IU 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 Pine Grove Area School District uses software purchased from the Central Susquehanna Intermediate Unit #16 (CSIU) for its critical student accounting applications (membership and attendance). The CSIU has remote access into the District's network servers.

Based on our current year 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 they are adequately monitoring all CSIU activity in their system. However, since the District has manual compensating controls in place to verify the integrity of the membership and attendance information in its database, that risk is mitigated. Membership reconciliations are performed between manual records and reports generated from the Student Accounting System.

Reliance on manual compensating controls becomes increasingly problematic if the District would ever move into an entirely paperless future with decentralized direct entry of data into their systems. Unmonitored CSIU 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 found the District had the following weaknesses over CSIU access to the District's system:

1. The District does not have a formal contract with the CSIU to provide student accounting applications and related information technology services.

2. The District's Acceptable Use Policy does not include provisions for authentication (password security and syntax requirements).

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

4. The District does not require written authorization before adding, deleting, or changing a userID.

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

6. The District has certain weaknesses in logical access controls. We noted that the District's system parameter settings do not require all users, including the IU, to log off the system after a period of inactivity (i.e., 60 minutes maximum) and also does not maintain a password history to prevent the use of a repetitive password (i.e., approximately last ten passwords).

7. The CSIU uses a group userID rather than requiring that each employee has a unique userID and password.

8. The CSIU has unlimited access (24 hours a day/7 days a week) into the District's system.

9. The District does not have evidence they are generating or reviewing monitoring reports of user access and activity on the system (including IU and District employees). There is no evidence that the District is performing procedures in order to determine which data the CSIU may have altered or which CSIU employees accessed their system.

10. The District/CSIU is not using the most current version of the remote access software.

11. The District has not enabled all security features of its remote access software. The District does not use encryption to secure the District's remote connections.

12. 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.

13. The District does not maintain the servers with membership/attendance data in a restricted/secure area. The servers are located in the payroll coordinator's office which is open during the normal working hours.

14. The District does not have a list of personnel with authorized access to the area where the servers with the membership/attendance data reside.

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

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

Recommendations

The *Pine Grove Area School District* should:

1. Develop an agreement with the CSIU to provide student accounting applications and related information technology services. The agreement should cover legal, financial, organizational, documentary, performance, security, intellectual property, and termination responsibilities and liabilities (including penalty clauses). All contracts and contract changes should be reviewed by legal advisors.

2. Ensure that the District's Acceptable Use Policy includes provisions for authentication (password security and syntax requirements).

3. Establish separate IT policies and procedures for controlling the activities of the CSIU and have the CSIU sign this policy, or the District should require the CSIU to sign the district's Acceptable Use Policy.

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

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

6. Implement a security policy and system parameter settings to require all users, including the CSIU, to log off the system after a period of inactivity (i.e., 60 minutes maximum). In addition, the District should implement a security policy and system parameter settings to maintain a password history that will prevent the use of a repetitive password (i.e., last ten passwords).

7. Require the CSIU to assign unique userIDs and passwords to vendor employees authorized to access the District system. Further, the District should obtain a list of CSIU employees with access to its data and ensure that changes to the data are made only by authorized vendor representatives.

8. Only allow access to their system when the CSIU needs access to make pre-approved changes/updates or requested assistance. This access should be removed when the CSIU has completed its work. This procedure would also enable the monitoring of CSIU changes.

9. Generate monitoring reports (including firewall logs) of CSIU and employee access and activity on their system. Monitoring reports should include the date, time, and reason for access, change(s) made and who made the change(s). 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.

10. Upgrade the remote access software to the most current version.

11. Encrypt the District's remote connections.

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

13. Maintain the servers with the membership/attendance data in a restricted/secure area in order to detect/deter unauthorized physical access to the membership/attendance data.

14. Develop and maintain a list of authorized individuals with access to the hardware (servers) that contains the membership/attendance data.

15. 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 detectors / install fire extinguishers in the computer room.

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

Management Response

Management stated the following:

1. The District has contacted CSIU – IU16 requesting a copy of the original formal contract for the IU to provide the District with student applications and related information technology services.

2. The District will append the current Acceptable Use Policy to include a provision for authentication (password security and syntax requirements).

3. The District will require CSIU – IU16 employees to sign our AUP and in addition the District will create a policy, or append our current AUP, to have policies and procedures in place to control the activities of CSIU – IU16 employees.

4. The District will develop a procedure to provide require written authorization before adding, deleting, or changing a userID.

5. The District will develop a procedure to maintain proper documentation to evidence that terminated employees were removed from the system in a timely manner.

6. The District will recommend to CSIU – IU16 that the system has a feature that will allow automatic logoff after a period of user inactivity. The District has implemented a system of maintaining password history to prevent the use of repetitive password (i.e., at least last ten passwords).

7. The District will continue to use 1 userID for CSIU – IU16 but turn off the user account unless a remote session is required. In addition, the District will log the name of the CSIU – IU16 employee along with the date and time of their access.

8. The District will turn off access to the CSIU – IU16 account unless remote access to our system is required by CSIU – IU16 personnel.

9. The District will turn on access logging in the CSIU – IU16 application software to monitor user access and activity on the system.

10. The District is currently using Windows XP for remote access. XP is at its life cycle end and is being replaced with Windows 7. When the District migrates to Windows 7, the remote access will be updated.

11. The District is currently using Windows XP for remote access. XP is at its life cycle end and is being replaced with Windows 7. When the District migrates to Windows 7, the remote access will be updated.

12. The District depends on CSIU – IU16 to analyze the impact of proposed program changes in relation to other business-critical functions.

13. Currently the District has no other place to house the server that maintains the membership and attendance data. In the future the District will need to look at building a computer room to house servers. The computer room will then be limited to authorized personnel and would have environmental and fire detection and suppression equipment installed.

14. Currently the District has no other place to house the server that maintains the membership and attendance data. In the future the District will need to look at building a computer room to house servers. The computer room will then be limited to authorized personnel and would have environmental and fire detection and suppression equipment installed.

15. Currently the District has no other place to house the server that maintains the membership and attendance data. In the future the District will need to look at building a computer room to house servers. The computer room will then be limited to authorized personnel and would have environmental and fire detection and suppression equipment installed.

16. Currently the District transports backup tapes off site with the Assistant Business Manager. The Assistant Business Manager places the backup tapes in a fireproof save in her home. The District will look at renting data storage space from IU29 and transfer data electronically to the offsite location.

Status of Prior Audit Findings and Observations

Our prior audit of the Pine Grove Area School District (PGASD) for the school years 2005-06 and 2004-05 resulted in one reported observation. The observation pertained to the District not maintaining an updated Memorandum of Understanding (MOU). As part of our current audit, we determined the status of corrective action taken by the District to implement our prior recommendations. We performed audit procedures, and questioned District personnel regarding the prior observation. As shown below, we found that the PGASD did implement recommendations related to our prior observation regarding the District not maintaining an updated Memorandum of Understanding.

School Years 2005-06 and 2004-05 Auditor General Performance Audit Report		
Prior Recommendations	**Implementation Status**	
I. Observation: Memorandum of Understanding Not Updated Timely 1. Review, update and re-execute the current Memorandum of Understanding (MOU) between the District and the Pine Grove Borough Police Department. 2. Adopt a policy requiring the administration to review and re-execute the MOU every two years.	**Background**: Our prior audit of the District's records found that the current MOU between the District and the Pine Grove Borough Police Department signed September 18, 1998 has not been updated.	*Current Status*: We followed up on the PGASD's MOU and found that the District <u>did</u> take corrective action to address our prior audit recommendations. The PGASD provided a current and fully executed MOU between the District and the Pine Grove Borough Police Department signed April 6, 2009.

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 Edward G. Rendell
Governor
Commonwealth of Pennsylvania
Harrisburg, PA 17120

The Honorable Gerald Zahorchak, D.Ed.
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

Senator Jeffrey Piccola
Chair
Senate Education Committee
173 Main Capitol Building
Harrisburg, PA 17120

Senator Andrew Dinniman
Democratic Chair
Senate Education Committee
183 Main Capitol Building
Harrisburg, PA 17120

Representative James Roebuck
Chair
House Education Committee
208 Irvis Office Building
Harrisburg, PA 17120

Representative Paul Clymer
Republican Chair
House Education Committee
216 Ryan Office 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.