

CONNELLSVILLE AREA SCHOOL DISTRICT  
FAYETTE COUNTY, PENNSYLVANIA  
PERFORMANCE AUDIT REPORT

SEPTEMBER 2010



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

Mr. Kevin Lape, Board President  
Connellsville Area School District  
732 Rockridge Road  
Connellsville, Pennsylvania 15425

Dear Governor Rendell and Mr. Lape:

We conducted a performance audit of the Connellsville Area School District (CASD) to determine its compliance with applicable state laws, regulations, contracts, grant requirements and administrative procedures. Our audit covered the period November 5, 2007 through February 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 CASD 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 CASD's management and their responses are included in the audit report. We believe the implementation of our recommendations will improve CASD's operations and facilitate compliance with legal and administrative requirements. We appreciate the CASD's cooperation during the conduct of the audit and their willingness to implement our recommendations.

Sincerely,

/s/

JACK WAGNER  
Auditor General

September 20, 2010

cc: **CONNELLSVILLE AREA SCHOOL DISTRICT** Board Members

## **Table of Contents**

---

---

	Page
Executive Summary .....	1
Audit Scope, Objectives, and Methodology .....	3
Findings and Observations .....	6
Observation – Unmonitored Vendor System Access and Logical Access Control Weaknesses .....	6
Status of Prior Audit Findings and Observations .....	10
Distribution List .....	15



## **Executive Summary**

---

---

### **Audit Work**

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

Our audit scope covered the period November 5, 2007 through February 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 CASD encompasses approximately 20 square miles. According to 2000 federal census data, it serves a resident population of 38,303. According to District officials, in school year 2007-08 the CASD provided basic educational services to 5,127 pupils through the employment of 370 teachers, 248 full-time and part-time support personnel, and 20 administrators. Lastly, the CASD received more than \$41.4 million in state funding in school year 2007-08.

### **Audit Conclusion and Results**

Our audit found that the CASD 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 CASD's data could occur and not be detected because the CASD was unable to provide supporting evidence that it is adequately monitoring all vendor activity in its system (see page 6).

#### **Status of Prior Audit Findings and**

**Observations.** With regard to the status of our prior audit recommendations to the CASD from an audit we conducted of the 2005-06 and 2004-05 school years, we found the CASD had taken appropriate corrective action in implementing our recommendations pertaining to errors in reporting nonresident membership (see page 10), insufficient documentation to support reported resident pupil membership data (see page 11), and errors in reporting health services data (see page 11).

We found the CASD had not taken appropriate corrective action in implementing our recommendations pertaining to unmonitored vendor system access and logical access control weaknesses (see page 12).





## 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 November 5, 2007 through February 22, 2010, except for the review of outside vendor access to the District's student accounting applications which was completed on March 4, 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 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 CASD'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:

- ✓ In areas where the District receives state subsidy and reimbursements based on pupil membership (e.g. basic education, special education, and vocational education), did it follow applicable laws and procedures?
- ✓ 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

### *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 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.

CASD 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 and financial stability.
- Items such as Board meeting minutes, pupil membership records, and reimbursement applications.

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

Lastly, to determine the status of our audit recommendations made in a prior audit report released on December 18, 2008, we performed audit procedures targeting the previously reported matters.

## Findings and Observations

---

### Observation

---

*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.

### Unmonitored Vendor System Access and Logical Access Control Weaknesses

Beginning in April 2009, the Connellsville Area School District obtained services from an outside vendor for technical support for its critical student accounting applications (membership and attendance). The technical support vendor 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 it is adequately monitoring all vendor activity in its system. This is a continuation of an observation included in our prior audit report (see page 12). However, since our prior audit report, the District has instituted adequate manual compensating controls to verify the integrity of the membership and attendance information in its database, so 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 found the District had the following weaknesses over vendor access to the District’s system:

1. The District does not have evidence that it is reviewing monitoring reports of user remote 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 their system.

2. The vendor uses a group userID rather than requiring that each employee has a unique userID and password.
3. The vendor has unlimited remote access (24 hours a day/7 days a week) into the District's system.
4. The District does not maintain proper documentation to evidence that terminated employees were removed from the system in a timely manner.
5. The District was unable to provide evidence that it requires written authorization for adding, deleting or changing a userID.
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 authentication (e.g., password security and syntax requirements) and privacy (monitoring of electronic mail, access to files).
8. 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 vendor, to change their passwords every 30 days; to use passwords that are a minimum length of eight characters and include alpha, numeric and special characters; to maintain a password history (i.e., approximately ten passwords). Additionally, the District could not provide evidence that the District's system parameter settings require all users, including the vendor, to lock out users after three unsuccessful attempts and to log off the system after a period of inactivity (i.e., 60 minutes maximum).

## **Recommendations**

The *Connellsville Area School District* should:

1. Generate monitoring reports (including firewall logs) of the vendor and employee remote access and activity on its 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.

2. Require the vendor to assign unique userIDs and passwords to vendor employees authorized to access the District system. Further, the District should ensure that changes to the data are made only by authorized vendor representatives.
3. Allow remote access to the system only when the vendor needs access to make pre-approved changes/updates or requested assistance. This access should be removed when the vendor has completed its work. This procedure would also enable the monitoring of vendor changes.
4. Maintain documentation to evidence that terminated employees are properly removed from the system in a timely manner.
5. Develop policies and procedures to require written authorization when adding, deleting, or changing a userID.
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 in its Acceptable Use Policy provisions for authentication (e.g., password security and syntax requirements) and privacy (monitoring of electronic mail, access to files).
8. Implement a security policy and system parameter settings to require all users, including the vendor, to change their passwords on a regular basis (i.e., every 30 days). Passwords should be a minimum length of eight characters and include alpha, numeric, and special character. The District should maintain a password history that will prevent the use of a repetitive password (i.e., last ten passwords). Also, the District should provide documentation, e.g. screen shots, that evidence that the system parameter settings require all users, including the vendor, to lock out users after three

unsuccessful attempts; and log users off the system after a period of inactivity (i.e., 60 minutes maximum).

**Management Response**

Management stated the following:

We have met with our District technology consulting firm and will be moving on the recommendations in the near future.

## Status of Prior Audit Findings and Observations

Our prior audit of the Connellsville Area School District (CASD) for the school years 2005-06 and 2004-05 resulted in three reported findings and one observation, as shown in the following table. 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 findings and observation. As shown below, we found that the CASD did implement recommendations related to our prior audit report's findings, but failed to implement our recommendations in the observation regarding vendor system access and logical access controls.

<i>School Years 2005-06 and 2004-05 Auditor General Performance Audit Report</i>		
<i>Prior Recommendations</i>	<i>Implementation Status</i>	
<p><u><i>I. Finding No. 1: Errors in Reporting Nonresident Membership Resulted in Overpayments of \$40,957 in Tuition for Children Placed in Private Homes</i></u></p> <ol style="list-style-type: none"> <li>1. Review membership data thoroughly to ensure students are properly classified prior to submitting reports to the Department of Education (DE).</li> <li>2. Review reports submitted subsequent to the years audited, and submit revised reports to DE if errors are found.</li> <li>3. DE should adjust the District's allocations to recover the overpayments of \$40,957 in tuition for children placed in private homes.</li> </ol>	<p><b>Background:</b></p> <p>Our prior audit of pupil membership reports submitted to DE for the 2005-06 and 2004-05 school years found that nonresident membership for children placed in private homes was overstated for both years. The errors resulted in overpayments of \$21,062 and \$19,895 in tuition for children placed in private homes for the 2005-06 and 2004-05 school years, respectively.</p>	<p><b>Current Status:</b></p> <p>Our current audit of pupil membership reports for the 2007-08 and 2006-07 school years found that nonresident membership for children placed in private homes was correctly reported to DE. We therefore concluded that the District did take corrective action to address this finding.</p> <p>As of completion of our fieldwork, DE had not yet adjusted the District's allocations. Therefore, we again recommend that DE do so to recover the overpayments of \$40,957.</p>



<p><u>II. Finding No. 2: Insufficient Documentation to Support Reported Resident Pupil Membership Data and Related Reimbursements</u></p> <ol style="list-style-type: none"> <li>1. Establish procedures to retain membership data in a format that fulfills DE's requirements.</li> <li>2. Maintain relevant computer printouts.</li> </ol>	<p><b>Background:</b></p> <p>Our prior audit of the District's child accounting data for the 2005-06 school year found that the District had insufficient documentation to support reported pupil membership data, resulting in our inability to verify the District's entitlement to various subsidies.</p>	<p><b>Current Status:</b></p> <p>Our current audit of child accounting data for the 2006-07 school year found that the District had sufficient documentation. We were able to audit pupil membership and verify the District's entitlement to various subsidies. We therefore concluded that the District did take corrective action to address this finding.</p>
--	--	---

<p><u>III. Finding No. 3: Errors in Reporting Health Services Data</u></p> <ol style="list-style-type: none"> <li>1. Reconcile the membership reports for career and technology center students to the health services reimbursements application, to ensure correct reporting of average daily membership (ADM).</li> <li>2. Report ADM only for those intermediate unit students receiving health services from the District.</li> <li>3. The Department of Health (DH) should adjust the District's health services reimbursement to resolve the reimbursement underpayments of \$3,445.</li> </ol>	<p><b>Background:</b></p> <p>Our prior audit of the District's health services reimbursement data for the 2004-05 school year found an error in reporting ADM to DH, resulting in underpayments of \$3,445.</p>	<p><b>Current Status:</b></p> <p>Our current audit of the District's health services reimbursement data for the 2007-08 and 2006-07 school years found that the District correctly reported ADM to DH. We therefore concluded that the District did take corrective action to address this finding.</p> <p>As of completion of our fieldwork, DH had not yet adjusted the District's reimbursement. Therefore, we again recommend that DH do so to resolve the underpayments of \$3,445.</p>
--	---	--

<i><b>IV. Observation:</b></i>	<b>Background:</b>	<i><b>Current Status:</b></i>
<p><i><u>Unmonitored Vendor System Access and Logical Access Control Weaknesses</u></i></p> <ol style="list-style-type: none"> <li>1. Generate monitoring reports (including firewall logs) of the vendor and employee remote access and activity on their system.</li> <li>2. Perform reconciliations between system generated membership and attendance reports and manually kept membership and attendance records.</li> <li>3. Require the vendor to assign unique userIDs and passwords to vendor employees authorized to access the District system.</li> <li>4. Allow remote access to the system only when the vendor needs access to make pre-approved changes/updates or requested assistance.</li> <li>5. Include a non-disclosure agreement for the District's proprietary information in the contract with the vendor.</li> <li>6. Maintain documentation to evidence that terminated employees are properly removed from the system in a timely manner.</li> <li>7. Allow upgrades/updates to the District's system only after written authorization from appropriate District officials.</li> </ol>	<p>Our prior audit of CASD found 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.</p>	<p>In April 2009, the District changed software vendors and now contracts with an outside vendor for its technical support. Our current review of the District's critical applications found that eight weaknesses still exist. We therefore concluded that the District did not take corrective action to address this observation. (See the current observation beginning on page 6.)</p>

<p>8. Store back-up tapes in a secure, off-site location.</p> <p>9. 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.</p> <p>10. Include in its Acceptable Use Policy provisions for authentication and privacy.</p> <p>11. Establish policies and procedures to analyze the impact of proposed program changes in relation to other business-critical functions.</p> <p>12. Implement a security policy and system parameter settings to require all users, including the vendor to change their passwords on a regular basis. Passwords should be a minimum length and include alpha, numeric, and special characters. The District should maintain a password history that will prevent the use of a repetitive password and lock out users after three unsuccessful attempts.</p> <p>13. 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.</p>		
--	--	--



## **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](http://www.auditorgen.state.pa.us), and the following:

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

The Honorable Thomas E. Gluck  
Acting 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](http://www.auditorgen.state.pa.us).

