SHIPPENSBURG AREA SCHOOL DISTRICT

CUMBERLAND COUNTY, PENNSYLVANIA

PERFORMANCE AUDIT REPORT

DECEMBER 2010

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

Mr. Herbert Cassidy, Board President
Shippensburg Area School District
317 North Morris Street
Shippensburg, Pennsylvania 17257

Dear Governor Rendell and Mr. Cassidy:

We conducted a performance audit of the Shippensburg Area School District (SASD) to determine its compliance with applicable state laws, regulations, contracts, grant requirements and administrative procedures. Our audit covered the period August 14, 2007 through May 5, 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 SASD 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 SASD's management and their responses are included in the audit report. We believe the implementation of our recommendations will improve SASD's operations and facilitate compliance with legal and administrative requirements.

Sincerely,

/s/
JACK WAGNER
Auditor General

December 9, 2010

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

Table of Contents

JACK WAGNER

AUDITOR GENERAL

Executive Summary

Audit Work

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

Our audit scope covered the period August 14, 2007 through May 5, 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 SASD encompasses approximately 121 square miles. According to 2000 federal census data it serves a resident population of 23,714. According to District officials, in school year 2007-08 the SASD provided basic educational services to 3,464 pupils through the employment of 235 teachers, 203 full-time and part-time support personnel, and 19 administrators. Lastly, the SASD received more than $13.8 million in state funding in school year 2007-08.

Audit Conclusion and Results

Our audit found that the SASD 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 SASD's data could occur and not be detected because the SASD 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 SASD from an audit we conducted of the 2005-06, 2004-05, 2003-04 and 2002-03 school years, we found the SASD had taken appropriate corrective action in implementing our recommendations pertaining to a school bus driver lacking a required clearance (see page 13) and board members failing to file Statements of Financial Interests (see page 14). Additionally, we found that the SASD no longer contracts with the vendor identified in our prior audit. As a result, the recommendations made regarding outside vendor access were no longer applicable (see page 14).

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 August 14, 2007 through May 5, 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 SASD'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:

✓ 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.

SASD 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 and pupil transportation.

Our audit examined the following:

- Records pertaining to bus driver qualifications, state ethics compliance, and financial stability.
- Items such as Board meeting minutes.

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

Lastly, to determine the status of our audit recommendations made in a prior audit report released on January 30, 2008, we performed 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 Shippensburg Area School District (SASD) uses software purchased from an outside vendor for its critical student accounting applications (membership and attendance). Additionally, the District's entire computer system, including all its data and the above vendor's software, are maintained on the vendor's servers, which are physically located at the vendor's site. The SASD has remote access into the vendor's network servers. The vendor also provides the District with system maintenance and support.

Based on our 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.

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.

We found the SASD had the following weaknesses over vendor access to the District's system:

1. The District's Acceptable Use Policy does not include provisions for authentication (password security and syntax requirements) and violations/incidents (what is to be reported and to whom).

2. SASD 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.

3. SASD 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 log off the system after a period of inactivity (i.e., 60 minutes maximum).

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

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

6. SASD 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 SASD is performing procedures to determine which data the vendor may have altered or which vendor employees accessed its system.

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

8. SASD does not have any compensating controls that would mitigate the IT weaknesses or alert the District to unauthorized changes to the membership database, i.e., reconciliations to manual records, analysis of membership trends, data entry procedures and review, etc.

Recommendations

The *Shippensburg Area School District* should:

1. Consider revising its Acceptable Use Policy to include provisions for authentication (password security and syntax requirements) and violations/incidents (what is to be reported and to whom).

2. 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.

3. Implement a security policy and system parameter settings to require all users, including the vendor, to log off the system after a period of inactivity (i.e., 60 minutes maximum).

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

5. Allow 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.

6. Generate monitoring reports (including firewall logs) of vendor 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). SASD should review these reports to determine that the access was appropriate and that data was not improperly altered. SASD should also ensure it is maintaining evidence to support this monitoring and review.

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

8. To mitigate IT control weaknesses, SASD should have compensating controls that would allow the District to detect unauthorized changes to the membership database in a timely manner.

Management Response

Management stated the following:

1. Board policy 815 will undergo an update to include information that better emphasizes password security and spells out that a password must be eight characters long, changed every 30 days, and that the user cannot reuse a password for seven changes. The updated policy will include information about the reporting of infractions and the consequences for infractions. The language used for the consequence section may be similar to what is already in the senior high student handbook explain the punishments for inappropriate technology usage.

2. [Vendor] employees are required to read and sign the [vendor] Global Business Conduct & Compliance Program. [The vendor] believes this document is sufficient to meet this need. With [the vendor's] employees not using district equipment, our acceptable use policy would have no affect on [Vendor] Public Sector employees except for when they are in the district providing training. The district will require them to sign our AUP when they come on site for training.

   If necessary, [the vendor] agreed to review the district's AUP for possible signature. . . .

3. The district would need to change vendors to comply with this recommendation. [The Vendor] agreed with this weakness and here is their response: "The [software] application uses the Basic Authentication model for authenticating user sessions. This model stores authentication information in the browser setting and resends the authentication with each page request. Because the authentication is handled locally by the browser on the user's PC, there are no server side controls that can be set to timeout sessions. The session ends when the user closes down the browser window from which the application was launched. Moving to a different authentication model is something the application development group is looking at."

4. Originally, a customer service representative answered the question about the unique login information. The district reviewed the applicable weaknesses/recommendations with a higher-level [vendor] employee. His response: "Support access to the ASP/SaaS [Application Service Provider/ Software as a Service] servers at the system level now requires users to log in with a unique user id. There are currently 163 unique user accounts set up for Support staff in addition to the 7 members of the ASP team. The list of users is not static and can be expected to change over time as staff are added, deleted, or reassigned. [The vendor] can provide a current list of users with accounts on request.

   "Logins to the ASP/SaaS environment by support users are used to support all of the customers in the ASP/SaaS environment. As such, all support users that need access to support any SaaS customer are set up on the ASP/SaaS systems for access."

   When asked about the inconstancy he elaborated: "My references are for system level access – basically, any user that needs to log directly onto the servers that are used in the hosting environment. All of those access operations are by unique user id. The users must log in through a gateway server that logs the users logins and logouts as well as other activities.

   "There is a "support" user account that is set up in the application security. That account is used for trainers and customer services folks when they need to run the application and see what the end user sees. All activity that occurs through the application interface, including for the support account, can be logged with the audit capabilities of the application. " . . .

5. With a hosted solution, this is not possible. If the district must remedy this recommendation, the district would need to go away from the hosted solution. Here is [the Vendor's] response: "It is also important to note that [the vendor] ASP/SaaS environment is used to provide ASP/SaaS services to a large number of school districts and municipalities. The servers and the infrastructure supporting the ASP/SaaS customers are

owned and maintained by [the vendor's] staff. It is not possible to limit access to the systems to specific times as the access is needed continuously to support and maintain the systems for all SaaS customers. [Vendor's] role as system administrators is one of the primary benefits of the ASP/SaaS offering and is integral to providing the service we offer."

6. With a hosted solution, this is not possible. If the district must remedy this recommendation, the district would need to go away from the hosted solution. Here is [the vendor's] response: "Activity performed by the customer support group including activities affecting data are logged in cases tracked in our call tracking system – First Wave. Activity from the hosting group-such as application update installation and system maintenance activities are reported on the application hosting start page calendar. The calendar and all case information are reviewable by the customer on-line. All [software] Application data that is changed while logged in to the application can be recorded with audit capabilities within the application. The district can use the [software] Reporting tools to generate reports of the audit data. The district may also establish an internal review process of membership data to verify that the information is accurate on a regular basis."

   If the district is able to stay with a hosted solution, the scheduling of training on how to review the audit data will occur.

7. There is no formal policy or procedure on program changes. With the current software, most changes are building specific and when the system was setup, the principals delegated responsibility to an implementation team. The Assistant Superintendent approves changes that affect more than one building. The district will create a policy identifying the position responsible for the separate areas in the building configurations, who is responsible to approve those changes, and who authorizes district or multi-building program changes.

8. The district will create a procedure to verify membership data. One possible solution would require building secretaries to print the [vendor] screen showing the date, total attendance, and total membership weekly. The secretaries could list the names of students that enrolled and withdrew from the building since the last report. The principal would sign the report and send them electronically to a central repository accessible by the person in charge of child accounting.

Auditor Conclusion

Due to the sensitive nature of the information in the system, we recommend that SASD evaluate the vendor's responses and determine what corrective action the District will need to take.

Status of Prior Audit Findings and Observations

Our prior audit of the Shippensburg Area School District (SASD) for the school years 2005-06, 2004-05, 2003-04 and 2002-03 resulted in two reported findings and one observation. The first finding pertained to a school bus driver who lacked a required clearance, and the second finding pertained to Statements of Financial Interest. The observation pertained to unmonitored vendor system access. 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 the observation. As shown below, we found that the SASD did implement recommendations related to the bus driver qualifications finding and the Statements of Financial Interests finding. We further noted that because the SASD changed software vendors our specific recommendations regarding unmonitored vendor system access and logical access control weaknesses were no longer applicable.

School Years 2005-06, 2004-05, 2003-04 and 2002-03 Auditor General Performance Audit Report		
Prior Recommendations	**Implementation Status**	
<u>I. Finding No. 1: School District Bus Driver Lacked Required Clearance</u> 1. Ensure that the District's transportation coordinator review each driver's qualifications prior to that person transporting students. 2. Work with the District's contractors to ensure that the District's bus driver files are up-to-date and complete.	**Background**: Our prior audit of bus driver qualifications for contracted drivers employed to transport District students found that one driver failed to have the required child abuse clearance as required by law. The District obtained the clearance after our audit found the deficiency.	***Current Status***: Our current audit found that all drivers we tested had the necessary qualifications to transport students. In February 2008, the transportation coordinator implemented a procedure to review each driver's qualifications before allowing them to transport students. In addition, all drivers are required to present a valid driver's license and annual physical form at the District office. The District obtains copies of these documents to ensure each driver's file is complete prior to submission to the board for approval to transport District students.

II. Finding No. 2: Board Members Failed to File Statements of Financial Interests According to Provisions of the Public Official and Employee Ethics Act 1. Seek the advice of the District's solicitor in regard to the board's responsibility when an elected or former board member fails to file a Statement of Financial Interests. 2. Develop procedures to ensure that all individuals required to file Statements of Financial Interests do so in compliance with the Ethics Act.	**Background**: Our prior audit of the District's Statements of Financial Interests for the years ended December 31, 2006, 2005, 2004 and 2003 found that three board members failed to file their statements for the 2003 year.	***Current Status*:** In January 2008 the business administrator consulted with the solicitor regarding the board's responsibility to file statements timely. Our current audit found that all board members filed their Statements of Financial Interests. Beginning with the 2007 calendar year the District implemented a checklist to ensure that all board members file their Statements of Financial Interests timely.

III. Observation: Unmonitored Vendor System Access and Logical Access Control Weaknesses 1. Generate monitoring reports (including firewall logs) of the vendor and employee remote access and activity on the 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.	**Background**: Our prior audit found that the District used software purchased from an outside vendor for its critical student accounting applications (membership and attendance). The software vendor had remote access into the District's network servers. 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.	***Current Status*:** Subsequent to our prior audit, the contract with the vendor was terminated. Therefore, our specific recommendations were no longer applicable. However, our current audit of controls covering the new contractor again found weaknesses, and resulted in the recommendations contained in the observation in our current audit report (see page 6).

2. Require the vendor to assign unique userIDs and passwords to vendor employees authorized to access the District's 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 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. 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 characters. Also, the District should maintain a password history that will prevent the use of a repetitive password (i.e., last ten passwords) and lock out users after three unsuccessful attempts. 8. Maintain the servers with membership/attendance data in a restricted/secure area in order to detect/deter unauthorized physical access to the membership/attendance data. 9. 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 and fire extinguishers in the computer room.		

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 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.

JACK WAGNER • AUDITOR GENERAL •