SCHOOL DISTRICT OF SPRINGFIELD TOWNSHIP

MONTGOMERY COUNTY, PENNSYLVANIA

PERFORMANCE AUDIT REPORT

JANUARY 2010

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

Mr. Malcolm Gran, Board President
School District of Springfield Township
1901 East Paper Mill Road
Oreland, Pennsylvania 19075

Dear Governor Rendell and Mr. Gran:

We conducted a performance audit of the School District of Springfield Township (SDST) to determine its compliance with applicable state laws, regulations, contracts, grant requirements and administrative procedures. Our audit covered the period June 27, 2006 through June 8, 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, 2007, 2006 and 2005. 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 SDST 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 SDST's management and their responses are included in the audit report. We believe the implementation of our recommendations will improve SDST's operations and facilitate compliance with legal and administrative requirements. We appreciate the SDST's cooperation during the conduct of the audit and their willingness to implement our recommendations.

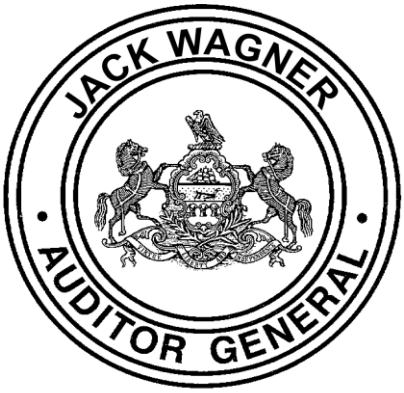
Sincerely,

/s/
JACK WAGNER
Auditor General

January 15, 2010

cc: **SCHOOL DISTRICT OF SPRINGFIELD TOWNSHIP** 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 School District of Springfield Township (SDST). 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 SDST in response to our prior audit recommendations.

Our audit scope covered the period June 27, 2006 through June 8, 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, 2006-07, 2005-06 and 2004-05.

District Background

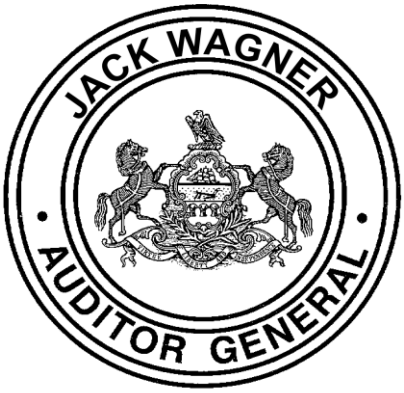
The SDST encompasses approximately 7 square miles. According to 2000 federal census data, it serves a resident population of 19,533. According to District officials, in school year 2007-08 the SDST provided basic educational services to 2,058 pupils through the employment of 183 teachers, 225 full-time and part-time support personnel, and 18 administrators. Lastly, the SDST received more than $4.3 million in state funding in school year 2007-08.

Audit Conclusion and Results

Our audit found that the SDST 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 Control Weaknesses. Based on our current year procedures, we determined that a risk exists that unauthorized changes to the SDST's data could occur and not be detected because the SDST was unable to provide supporting evidence that it's 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 SDST from an audit we conducted of the 2004-03 and 2003-02 school years, we found the SDST did not have any prior findings or observations (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 June 27, 2006 through June 8, 2009, except for the verification of professional employee certification which was performed for the period June 27, 2006 through May 4, 2009.

Regarding state subsidy and reimbursements, our audit covered school years 2007-08, 2006-07, 2005-06 and 2004-05.

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 SDST'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?

- ✓ 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?

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.

- ✓ In areas where the District receives state subsidy and reimbursements based on payroll (e.g. Social Security and retirement), did it follow applicable laws and procedures?
- ✓ 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?
- ✓ Does the District ensure that Board members appropriately comply with the Public Official and Employee Ethics Act?
- ✓ 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 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.

SDST 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 pupil transportation, bus driver qualifications, professional employee certification, state ethics compliance, and financial stability.
- Items such as Board meeting minutes, pupil membership records, and reimbursement applications.
- Deposited state funds.

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

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 School District of Springfield Township 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 location. The District 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. 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. Attendance and membership reconciliations are performed between manual records and reports generated from the student information system (SIS).

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

2. 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 AUP.

3. 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 use passwords that include alpha, numeric and special characters.

4. 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).

5. We noted that the District's system parameter settings do not lock out users after three unsuccessful access attempts.

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

7. 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 their system.

Recommendations

The *School District of Springfield Township* should:

1. Include in its AUP provisions for authentication (password security and syntax requirements).

2. Establish separate IT policies and procedures for controlling the activities of vendor/consultants and have the vendor sign this policy, or the District should require the vendor to sign the District's AUP.

3. Implement a security policy and system parameters settings to require all users, including the vendor, to use passwords that include alpha, numeric and special characters.

4. 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).

5. Implement a security policy and system parameter settings to lock out users after three unsuccessful access attempts.

6. Allow access to its system only when the vendor needs 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.

7. 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). 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.

Management Response

Management and the District's vendor provided the following in response to our observations.

1. **Vendor Response**: The district can modify their AUP as needed. We will allow the district to set password policy rules for the user accounts on the . . . systems in the very near future. Our goal was to have this capability in place by June 1, 2009. We have missed the original target, but currently expect the capability to be in place by June 15, 2009.

   District Response: This recommendation will be made to our Board of School Director's Policy Committee for consideration once these controls are turned over to us by the vendor. We will implement the recommended syntax requirements at the start of the 2009-2010 school year.

2. **Vendor Response:** The district can establish IT policies and procedures as desired. [Vendor] employees are required read and sign the [vendor's] Business Conduct & Compliance Program. A copy of the form is available at the URL listed below. [The vendor] believes this document is sufficient to meet this need. However, if district wishes to have [the vendor] sign a copy of the districts AUP or vendor IT Security policies, [we] will review those documents for signature.
http://www.sungard.com/aboutsungard/corporateresponsibility.aspx

   In addition, [the vendor's] Bethlehem hosting offering is currently working toward obtaining a SAS [Statement on Auditing Standards]70 certification for its hosted offering. The audit firm KPGM has been engaged to perform the audit. The first SAS70 Level II audit report will be available around the end of the first quarter of 2010. The report will cover the period of July 1, 2009 through December 31, 2009. Following the initial report, we expect to recertify the offering on an annual basis.

   District Response: Although we believe that SAS70 certification, an accounting industry standard for auditing IT security processes, is sufficient, we will request that the vendor review and sign our Acceptable Use Policy prior to the start of the 2009-2010 school year.

3. **Vendor Response:** The district can establish security policies for its users. We intend to allow hosted districts to set password policy for the districts users in the very near future. Our goal was to have this capability in place by June 1, 2009. We have missed the original target, but currently expect the capability to be in place by June 15, 2009. The SaaS [Software as a Service] offering is managed by [the vendor] for more than 100 districts across the United States. [U]sers must comply with the . . . password policy detailed below. [The vendor] cannot commit to aligning its policy with that of any particular customer.

The minimum standards for password construction are as follows:

- New users will be given an initial password that will be valid for initial login only.
- Passwords must be at least eight (8) characters in length.
- Passwords must be a mix of letters, numbers and at least one upper case character.
- A minimum of twenty four (24) password history will be enforced.
- The minimum password age is three (3) days except for the initial password.
- A minimum lockout period of fifteen (15) minutes will be enforced after five (5) failed login attempts within 15 minutes on standard systems.
- Passwords or access codes for two-factor authentication systems must lockout permanently after five (5) failed login attempts within a 24-hour period.
- For normal users passwords will be set to automatically expire every 60 days.
- For administrators passwords will be set to automatically expire every 30 days.

District Response: We will align our password policies for access to our SIS with applicable standards outlined above.

4. **Vendor Response:** The [SIS] 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.

District Response: Although we maintain logout controls over many of our internal systems, we are unable to implement the recommended controls on the Basic Authentication model described above. Once vendor converts to a .net environment, we will establish controls locally to meet the recommendation.

5. **Vendor Response:** We will allow the district to set password policy rules for the user accounts on the . . . systems in the very near future. Our goal was to have this capability in place by June 1, 2009. We have missed the original target, but currently expect the capability to be in place by June 15, 2009.

   District Response: Once controls are turned over to us, we will implement recommendation. Assuming the June 15 deadline is met, we will have controls in place for the 2009-2010 school year.

6. **Vendor Response:** It is also important to note that because the [vendor] environment is used to provide SaaS services to a large number of school districts and municipalities. The servers and the infrastructure supporting the SaaS customers is 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.

   District Response: The recommendation assumes that the data is stored locally in the district and that we have direct control over their access. As indicated by the vendor, that is not the nature of a SaaS environment. However, we must approve requests from and schedule with the vendor to perform major upgrades to our software and database. Routine updates and patches are conducted by our vendor on a regular basis, as this is a significant advantage to the SaaS model.

7. **Vendor Response:** We cannot provide firewall or system logs. These contain confidential information and are not available for release. Now that we have moved to named user access, we will see if we can create a report of support user system access. Again the issue is that the vast majority of the support user logins to the SaaS system will not be to support a particular

district. Users will log in to support any of the more than 100 SaaS customers currently on the [vendor] Systems.

District Response: Vendor addressed the issue of firewall system logs and this proprietary information. We do conduct internal monthly audits of our attendance and membership records and can trace an error back to its source. However, we will investigate with our vendor any built-in automated auditing features and the feasibility of running more frequent spot checks of the recorded audit trails.

District General Response and Summary:

In 2006, we entered into an agreement with [the vendor] Application Hosting to provide us with [a SIS] in an Application Service Provider (ASP) environment. In short, [the vendor] provides the software as a service (SaaS) and store our database (which we own) from their hosting environment. We maintained at the time and still maintain that this is the most practical and secure solution for a small school district with limited staff resources. In fact, this is a growing trend among SIS and other information and instructional systems providers. [The vendor] is an international leader in data management and security. They offer significant advantages with regard to physical security of data, redundancy of power and server resources, backup and disaster recovery capabilities. They manage data for school districts and municipalities. Thus far, we have been satisfied with their reliability, uptime, management of updates and patches, and response to any concerns related to hosting. The tradeoff, of course, as highlighted by this audit, is that we do not have complete autonomy over processes and procedures inside of the hosting facility, only over our internal processes within the framework of the hosting environment. To our knowledge, there has been no breach in membership and attendance data security either through physical or logical means over the course of our relationship with [the vendor]. Further, we keep a tight rein on change permissions locally to this information and manually audit our attendance and membership data monthly which significantly mitigates

the risk of errors or unauthorized changes going un-noticed.

In light of the observations and recommendations, we felt it necessary to include [the vendor] in the process of formulating our response, as we require their assistance to implement those recommendations. We believe [the vendor] has provided dates for most of the needed changes sufficient for us to implement most recommendations for the 2009-2010 school year. Automated logout is not technically feasible for the 2009-2010 school year under current authentication protocols limited by the web browser interface but we do expect .net technology to address this concern once [the vendor] migrates to it. In the meantime, we will continue to educate faculty and administration regarding the need to manually logout when the system is not in use and/or they are not present.

In conclusion we believe our data is secure in the current SaaS environment. There has been no breach, compromise or violation of our attendance and membership data since moving to this environment, either physical of logical, and we have local protocols in place to mitigate the risks inferred in the report. However, we do not object to the implementation of most of the recommendations and as it becomes feasible to proceed, we will do so within a reasonable time frame and in accordance with our existing policies and processes.

Auditor Conclusion

Any recommendations implemented subsequent to our fieldwork complete date will be verified during our next audit.

Status of Prior Audit Findings and Observations

Our prior audit of the School District of Springfield Township for the school years 2003-04 and 2002-03 resulted in no findings or observations.

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

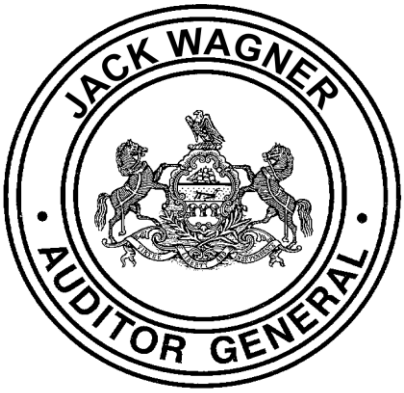
Representative James Roebuck
Chair
House Education Committee
208 Irvis Office Building
Harrisburg, PA 17120

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


JACK WAGNER
AUDITOR GENERAL

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.