SOUTHEAST DELCO SCHOOL DISTRICT

DELAWARE COUNTY, PENNSYLVANIA

PERFORMANCE AUDIT REPORT

OCTOBER 2009

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

Mr. Donald Young, Board President
Southeast Delco School District
1560 Delmar Drive
Folcroft, Pennsylvania 19032

Dear Governor Rendell and Mr.Young:

We conducted a performance audit of the Southeast Delco School District (SDSD) to determine its compliance with applicable state laws, regulations, contracts, grant requirements and administrative procedures. Our audit covered the period December 16, 2005 through February 20, 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, 2006, and June 30, 2005, as they were the most recent reimbursements subject to audit. 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 SDSD complied, in all significant respects, with applicable state laws, regulations, contracts, grant requirements, and administrative procedures, except as detailed in one finding noted in this report. In addition, we identified two matters unrelated to compliance that are reported as observations. A summary of these results is presented in the Executive Summary section of the audit report.

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

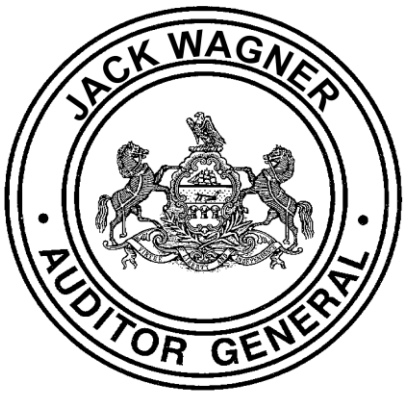
Sincerely,

/s/
JACK WAGNER
Auditor General

October 29, 2009

cc: **SOUTHEAST DELCO 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 Southeast Delco School District (SDSD). 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 SDSD in response to our prior audit recommendations.

Our audit scope covered the period December 16, 2005 through February 20, 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 2005-06 and 2004-05 as they were the most recent reimbursements subject to audit. The audit evidence necessary to determine compliance specific to reimbursements is not available for audit until 16 months, or more, after the close of a school year.

District Background

The SDSD encompasses approximately 5 square miles. According to 2000 federal census data, it serves a resident population of 38,208. According to District officials, in school year 2005-06 the SDSD provided basic educational services to 4,200 pupils through the employment of 290 teachers, 250 full-time and part-time support personnel, and 22 administrators. Lastly, the SDSD received more than $16.9 million in state funding in school year 2005-06.

Audit Conclusion and Results

Our audit found that the SDSD complied, in all significant respects, with applicable state laws, regulations, contracts, grant requirements, and administrative procedures, except for one compliance-related matter reported as a finding. In addition, two matters unrelated to compliance are reported as observations.

Finding: Internal Control Weaknesses Resulted in Our Inability to Verify $3,289,773 of State Funding. SDSD failed to retain documentation to support state funding for Social Security, the Educational Assistance Program, and certain other grants (see page 6).

Observation No. 1: Memorandum of Understanding Not Updated Timely. Our audit of SDSD's records found that the Memorandum of Understanding between SDSD and the Collingdale Police Department had not been updated since October 2005 (see page 9).

Observation No. 2: Unmonitored Vendor System Access and Logical Access Control Weaknesses. We determined that a risk exists that unauthorized changes to SDSD's child accounting data could occur and not be detected because SDSD was unable to provide supporting evidence that it is adequately monitoring all vendor activity in its system (see page 11).

Status of Prior Audit Findings and Observations. With regard to the status of our prior audit recommendations to the SDSD from an audit we conducted of the 2003-04 and 2002-03 school years, we found the SDSD had not taken corrective action in implementing our recommendations pertaining to the internal control weaknesses in child accounting for our current years of audit (see page 19).

However, we found the SDSD had taken appropriate corrective action in implementing our recommendations pertaining to the failure of board members to file Statements of Financial Interests (see page 20) and internal control weaknesses regarding bus drivers' qualifications (see page 21).

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 December 16, 2005 through February 20, 2009, except for the verification of professional employee certification, which was performed for the period November 11, 2005 through October 2, 2008.

Regarding state subsidy and reimbursements, our audit covered school years 2005-06 and 2004-05 because the audit evidence necessary to determine compliance, including payment verification from the Commonwealth's Comptroller Operations and other supporting documentation from the Department of Education (DE), is not available for audit until 16 months, or more, after the close of a school year.

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 DE reporting guidelines, we use the term school year rather than fiscal year throughout this report. A school year covers the period July 1 to June 30.

Objectives

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 SDSD'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?

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 pupil membership (e.g. basic education, special education, and vocational education), did it follow applicable laws and procedures?
- ✓ 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

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.

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

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

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

Our audit examined the following:

- Records pertaining to bus driver qualifications, professional employee certification, 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 SDSD operations.

Lastly, to determine the status of our audit recommendations made in a prior audit report released on April 5, 2006, we reviewed the SDSD's response to DE dated March 22, 2007. We then performed additional audit procedures targeting the previously reported matters.

Findings and Observations

Finding → **Internal Control Weaknesses Resulted in Our Inability to Verify $3,289,773 of State Funding**

Our audit of the Southeast Delco School District's (SDSD) files and records for the 2005-06 and 2004-05 school years found inadequate documentation to support state funding of $3,289,773, as follows:

Description	2005-06	2004-05	Totals
Social Security and Medicare	$1,041,633	$ 929,329	$1,970,962
Education Assistance Program	503,820	388,792	892,612
Extra Grants	426,199	-	426,199
Totals	$1,971,652	$1,318,121	$3,289,773

Criteria relevant to this finding:

Section 518 of the Public School Code requires that records be retained for a period of not less than six years.

Department of Education (DE) guidelines and instructions require the maintenance and retention of adequate documentation to verify the District's entitlement to state payments.

Social Security

District personnel could not provide Internal Revenue Service (IRS) Federal Form 941's (Employers' Quarterly Federal Tax Return) for the third quarter of 2005 and for the 2004-05 school year. As a result, we were unable to verify whether the District received the Commonwealth's matching share of Social Security and Medicare tax contributions to which it was entitled.

Good internal control procedures require the reconciliation of the IRS Federal Form 941 and the application for Social Security and Medicare reimbursement.

Educational Assistance Program (EAP)

District personnel could not provide receipts or final expenditure reports in support of the EAP payments for the 2005-06 and 2004-05 school years. As a result, we were unable to verify whether the District was entitled to receive these grants.

Extra Grants

District personnel could not provide any supporting documentation for $426,199 received as extra grants for the 2005-06 school year. As a result, we were unable to verify whether the District was entitled to receive these grants. The District did not receive any extra grants in 2004-05.

Internal controls are the responsibility of management. Good internal controls provide management with assurance that state funds have been correctly received and expended in accordance with the Department of Education guidelines and instructions. Weaknesses in internal controls do not provide management with those assurances. As a result of personnel turnover in the District's business office, documentation supporting state payments of $3,289,773 was not available for audit.

Recommendations

The *Southeast Delco School District* should:

1. Retain IRS federal forms to support the Social Security and Medicare reimbursements.

2. Maintain files for each program and grant containing the application, approval, budget and any revisions filed, documentation of receipt (such as a copy of the check transmittal and/or check), expenditure reports, invoices, purchases orders and documentation to support other requirements of the program.

The *Department of Education* should:

3. Require the District to maintain sufficient, competent, and relevant evidence to ensure proper justification for the receipt of state funds.

Management Response

Management stated the following:

1. The district was unable to provide supporting records for the 3rd quarter 941 Social Security filing for 2005. The district did request this information from the Internal Revenue Service and has not received a response as of this memo date. In addition, the district outsourced the payroll function in 2004-2005 and was unable to produce 941 filings for this time period.

2. Even though the district ledger recorded a significant portion of the expenditures for the educational assistance grant, a complete reconciliation and accounting of all expenditures required to support the subsidy from the state could not be produced. The district believes that with more time it could substantiate evidence of allowable spending of the grant monies. The district was also unable to produce a copy of the final expense reconciliation report for the grant and periods in question.

3. Although the extra grants were identified by the district, a complete reconciliation of the expenditures and final expenditure report for the grants in question could not be located in the district's archives.

Observation No. 1

Memorandum of Understanding Not Updated Timely

Our audit of the District's records found that the Memorandum of Understanding (MOU) between the District and the Collingdale Police Department was last signed and updated October 19, 2005.

The failure to update the MOUs with the local law enforcement agencies could result in a lack of cooperation, direction, and guidance between District employees and the law enforcement agencies if an incident occurs on school property, at any school-sponsored activity, or any public conveyance providing transportation to or from a school or school-sponsored activity. This internal control weakness could have an impact on law enforcement notification and response, and ultimately the resolution of a problem situation.

Criteria relevant to the observation:

Section 1303-A(c) of the Public School Code provides:

All school entities shall develop a memorandum of understanding with local law enforcement that sets forth procedures to be followed when an incident involving an act of violence or possession of a weapon by any person occurs on school property. Law enforcement protocols shall be developed in cooperation with local law enforcement and the Pennsylvania State Police.

The Basic Educational Circular (BEC) issued by the Department of Education entitled Safe Schools and Possession of Weapons, contains a sample MOU to be used by school entities. Section VI, General Provisions item B of this sample states:

This Memorandum may be amended, expanded or modified at any time upon the written consent of the parties, but in any event must be reviewed and re-executed within two years of the date of its original execution and every two years thereafter.

Recommendations

The *Southeast Delco School District* should:

1. Review, update and re-execute the MOU between the District and the Collingdale Police Department.

2. Adopt a policy requiring the administration to review and re-execute the MOU every two years.

Management Response

Management stated the following:

We take exception to the "Observation" which states, "Internal Control Weakness Regarding Updated Memorandum of Understanding." Our inability to get . . . local [law enforcement] to sign the updated memorandum does not constitute a weakness on the part of Southeast Delco School District. The district made numerous attempts to get the document signed without a positive result. The requirement for school districts to have a signed memorandum of understanding with local law enforcement agencies is squarely placed on the school district with no legislation requiring the same of the local agency. To penalize a school district, who has no ability to force compliance is actually a weakness in the enabling legislation not in the internal controls of the school district. The school district presented the updated memorandum to [local law enforcement] on 11/25/2008 for. . . signature. [Local law enforcement] wanted to have [its] solicitor review the memorandum. . . . [Local law enforcement] were spoken to by phone requesting the signed memorandum on 12/10/2008, 01/15/2009 and 02/10/2009 by [the] Southeast Delco School District Public Safety Coordinator. The superintendent's secretary also requested the signed memorandum, however we do not have a date of when that phone call was made.

Since the closing of the audit and at the time of this reply the memorandum was signed by [local law enforcement] on 03/03/2009 and a copy is attached [attachment not included here].

Auditor Conclusion

NOTE: Management's response refers to an earlier title of our draft observation, which we subsequently revised.

We appreciate the District's efforts to secure an updated MOU with the Collingdale Police Department. Because an updated MOU was provided, we modified the observation and changed the title to reflect this event. During our next audit we will determine whether the MOU is re-executed on or before March 3, 2011.

Observation No. 2

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 SDSD 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 software are maintained on the vendor's servers that are physically located at the vendor's site. The District has remote access into the vendor's network servers, with the vendor providing system maintenance and support.

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 activity in its system. Additionally, the District lacks sufficient manual compensating controls to verify the integrity of the membership and attendance information in its database. Since the District does not have adequate manual compensating controls in place, the risk of unauthorized changes is increased.

Best practices in information technology (IT) security include: limiting access to authorized users; ensuring individual accountability for actions; managing vendor services; monitoring the system to ensure integrity of key databases and applications; regulating changes to software; restricting physical access; implementing and maintaining minimum environmental controls; and planning for contingencies.

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

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

3. The District 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; and to maintain a password history (i.e., approximately ten passwords).

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

7. The District is unable to determine if the vendor is using the most current version of the remote access software.

8. The District is unable to determine if the vendor enables all security features of its remote access software. The District does not know if the vendor uses encryption to secure the remote connections.

9. The District did not provide requested documentation to evidence that security features are enabled in the remote access software.

10. The District does not require written authorization prior to the updating/upgrading of key applications.

11. The District does not have formal policies in place to control emergency changes to systems or programs.

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 is unable to determine if application(s) are backed up before placing program changes into production.

14. The District is unaware how the servers are being maintained and if the vendor is housing them in a restricted/secure area.

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

16. The District is unable to determine what environmental controls are in place in the room that contains the server that houses all of the District's data. We note that it is unknown if the specific location has fire detection, fire suppression equipment, and a temperature controlled room.

17. The District is unable to determine if the vendor performs regular backups of the system.

18. The District is unable to determine if the vendor stores data back-ups in a secure, off-site location.

19. The District does not have any compensating controls that would mitigate the IT weaknesses and would 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 *Southeast Delco School District* should:

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

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

3. 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).

4. Require the vendor to assign unique userIDs and passwords to vendor employees authorized to access the District's system. Further, the District 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 its system only when the vendor needs to make pre-approved changes/updates or provide 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 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.

7. Determine if the vendor is using the most current version of the remote access software.

8. Ensure that the vendor encrypts the remote connections.

9. Obtain documentation, e.g. screen shots, that evidence the remote access software security features are enabled.

10. Ensure that the upgrades/updates to the District's system are made only after receipt of written authorization from appropriate District officials.

11. Establish a process for defining, raising, testing, documenting, assessing and authorizing emergency changes to systems or programs that do not follow the established change process.

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

13. Determine if application(s) are being backed up before placing program changes into production to ensure they could be recovered if problems are encountered.

14. Ensure that the servers with the membership/attendance data are maintained in a restricted/secure area in order to detect/deter unauthorized physical access to the membership/attendance data.

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

16. 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 ensure that fire detectors and fire extinguishers are installed in the computer room. The District should also insure servers are kept in a temperature controlled room.

17. Ensure the vendor performs regular backups of the system.

18. Ensure the vendor stores back-up tapes in a secure, off-site location.

19. To mitigate IT control weaknesses, the District 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:

Having carefully read through the findings of the audit regarding technology controls of the Southeast Delco, I [the Director of Data and Technology Management] would like to respond to the issues addressed therein.

We are in agreement that there is no written form kept on file for adding, deleting or changing userIDs within the applications hosted both in house and off-site. While we do have a specific process outlined in our department, notification of any change comes through email from the Human Resources department. To address this finding we are in the process of creating a form which will be kept on file in the data offices for any addition, change, or deletion request. No requests absent this form will be honored.

Regarding changing of passwords, our financial package does require a password change every 30 days. Our information system is housed off campus, and we will inquire as to whether or not the system has the capability to automatically require password change. Absent that capability, we will create policy requiring application users to change passwords on a monthly basis.

The stated weakness regarding knowledge of a vendor using a group ID as opposed to a unique ID to enter the information system is unfounded. While it is true that our vendor enters our system through a support group ID, system protections on the vendors side document time, date and name of users entering the system. At any time we can request such if we have concerns about a compromise of the system.

It is true we cannot watch over the vendor's corrections, updates and fixes at every moment because we do not have the human resources to do so. It is for exactly that reason that we outsource our information system IT requirements as do hundreds of school district in the region. Access requiring prior notification by the district to the vendor in order to enter the system is done for major upgrades. On a daily basis, for troubleshooting, cases are logged and assigned to specific users and as such we create a notification and use trail. Remote access is encrypted. As such, all user access is in some form logged either in the application or on the server.

All information system applications are backed up on a nightly basis. Condition [#13] is unfounded. Programs changes in the information system do not affect the business functions since they are operating on non-communicating applications and such are populated separately. Condition [#12] is unfounded.

I am uncertain where you received the information for section [#14 through #18], but all of these statements are incorrect. As far as I know I was never asked to produce documentation regarding the housing of the information servers. It appears that it was listed as a matter of course.

While I respectfully understand the role this documentation plays, in order to have the total control you are suggesting in [#19], we would be required to house all of our applications including the student information system. To bring IT in house would require a significant yearly increase in our district budget. Not only would we need to hire IT support, but we would need staff to monitor daily entries through additional software or human resources.

I am not sure if your auditors have a clear understanding of the role played by off site vendors. If you are trying to relay that off site is less secure than on site, I would agree. Total 100% maximum security is certainly our goal. We must however operate within the financial constraints of our district.

Auditor Conclusion

As directed by the business manager, we conducted our IT procedures with the director of data management and the network administrator. All of the discrepancies cited in our observation were reviewed with these persons during field work and prior to writing the observation. Alternate procedures or evidence of alternate procedures were not disclosed to us at that time. Since we did not receive management's reply until after field work was completed, we will verify the District's assertions during our next scheduled audit. Meantime, the observation will stand as written.

Status of Prior Audit Findings and Observation

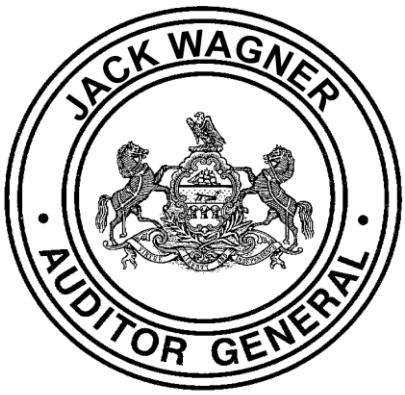
Our prior audit of the Southeast Delco School District (SDSD) for the school years 2003-04 and 2002-03 resulted in two reported findings and one observation. The first finding pertained to internal control weaknesses in child accounting, the second finding pertained to the failure of board members to file Statements of Financial Interests, and the observation pertained to internal control weaknesses regarding bus drivers' qualifications. As part of our current audit, we determined the status of corrective action taken by the District to implement our prior recommendations. We analyzed the SDSD Board's written response provided to the Department of Education (DE), performed audit procedures, and questioned District personnel regarding the prior findings. As shown below, we found that the SDSD had not yet implemented our recommendations related to internal control weaknesses in child accounting. However, SDSD did implement our recommendations related to the failure to file Statements of Financial Interests and internal control weaknesses regarding bus drivers' qualifications.

School Years 2003-04 and 2002-03 Auditor General Performance Audit Report		
Prior Recommendations	**Implementation Status**	
I. Finding No. 1: Internal Control Weaknesses in Child Accounting 1. Retain necessary documentation to support membership reported for all children placed in private homes. 2. Retain all documentation to support the membership reports. 3. Reconcile District records with the membership report for accuracy. 4. Properly report District average daily membership for health services reimbursement. 5. Adopt written procedures for the reporting and tracking of child accounting.	**Background**: Our prior audit of the District's child accounting data for the 2003-04 and 2002-03 school years found internal control weaknesses resulting in our inability to verify the District's entitlement to subsidies and reimbursements totaling $22,691,695.	***Current Status*:** Since our prior audit was not released until April 5, 2006, and the board did not officially reply to our recommendations until March 23, 2007, it was not possible for the SDSD to implement our recommendations for the current audit years (2005-06 and 2004-05). Documentation was still insufficient for us to verify the District's entitlement to subsidies and reimbursements based on child accounting data for those years. The effectiveness of the District's corrections will be verified during our next audit of the SDSD.

6. Institute internal control procedures to ensure child accounting data is accurate and supported by appropriate documentation prior to submission of final reports to DE.		

II. Finding No. 2: Board Members Failed to File Statements of Financial Interests in Violation of the Ethics Act 1. Seek the advice of the District's solicitor in regard to the board's responsibility when a member fails to file a Statement of Financial Interest. 2. Develop procedures to ensure that all individuals required to file Statements of Financial Interests do so in compliance with the Public Official and Employee Ethics Act.	**Background**: Our prior audit of the 2004, 2003 and 2002 calendar years' Statements of Financial Interests found that four board members failed to file for 2004, nine failed to file for 2003, and six failed to file for 2002. Additionally, one board member filed late for 2004 and another board member filed late for 2003. The District did not have a review process in place to ensure that all statements are filed when due.	***Current Status*:** Our current audit found that two board members failed to file their statements, and three filed their statements late, for the 2005 calendar year. The statements for the 2006 and 2007 calendar years were properly filed. As stated above, our prior audit was not released until April 5, 2006, and the board did not officially reply to our recommendations until March 23, 2007. It therefore was not possible for the SDSD to implement our recommendations for the 2005 calendar year. However, based on the results of our current audit, we concluded that the District did take appropriate corrective action for the subsequent years. Information concerning the failure to file the Statements of Financial Interests for 2005 will be forwarded to the State Ethics Commission for its review and determination of any further action.

III. Observation: Internal Control Weaknesses in Administrative Policies Regarding Bus Drivers' Qualifications 1. Develop a process to determine, on a case-by-case basis, whether prospective and current employees of the district have been charged with or convicted of crimes that, even though disqualifying under state law, affect their suitability to have direct contact with children. 2. Implement written policies and procedures to ensure the District is notified when drivers are charged with or convicted of crimes that call into question their suitability to continue to have direct contact with children.	**Background**: Our prior audit found that the District did not have written policies or procedures in place to ensure that it was notified if current employees were charged with or convicted of serious criminal offenses which should be considered for the purpose of determining an individual's continued suitability to be in direct contact with children. We considered this lack of written policies and procedures to be an internal control weakness that could result in the continued employment of individuals who may pose a risk if allowed to continue to have direct contact with children.	***Current Status*:** Our audit found that the District complied with our recommendations with the adoption of Policy No. 821 on March 27, 2008, requiring employees to immediately notifying the superintendent in writing of any offense reportable under specified state laws, any conviction of a criminal drug statute, or any felony conviction.


JACK WAGNER
AUDITOR GENERAL

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

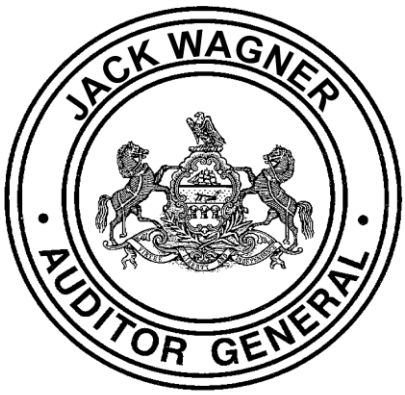
Representative James Roebuck
Chair
House Education Committee
208 Irvis Office Building
Harrisburg, PA 17120

Representative Paul Clymer
Republican Chair
House Education Committee
216 Ryan Office Building
Harrisburg, PA 17120

Ms. Barbara Nelson
Acting 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.