

SCHOOL DISTRICT OF HAVERFORD TOWNSHIP
DELAWARE COUNTY, PENNSYLVANIA
PERFORMANCE AUDIT REPORT

APRIL 2009

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

Mr. Denis A. Gray, Board President
School District of Haverford Township
1801 Darby Road
Havertown, Pennsylvania 19083

Dear Governor Rendell and Mr. Gray:

We conducted a performance audit of the School District of Haverford Township (SDHT) to determine its compliance with applicable state laws, regulations, contracts, grant requirements and administrative procedures. Our audit covered the period March 1, 2005 through August 4, 2008, 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, 2005, 2004 and 2003, 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 SDHT complied, in all significant respects, with applicable state laws, regulations, contracts, grant requirements, and administrative procedures. However, we identified three 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 observations and recommendations have been discussed with SDHT's management and their responses are included in the audit report. We believe the implementation of our recommendations will improve SDHT's operations and facilitate compliance with legal and administrative requirements

Sincerely,

/s/

JACK WAGNER
Auditor General

April 3, 2009

cc: **SCHOOL DISTRICT OF HAVERFORD TOWNSHIP** Board Members

Table of Contents

	Page
Executive Summary	1
Audit Scope, Objectives, and Methodology	3
Findings and Observations	7
Observation No. 1 – Unmonitored Vendor System Access and Logical Access Control Weaknesses	7
Observation No. 2 – Internal Control Weaknesses in Administrative Policies Regarding Bus Drivers’ Qualifications	12
Observation No. 3 – Internal Control Weakness Regarding Memorandum of Understanding	14
Status of Prior Audit Findings and Observations	16
Distribution List	17



Executive Summary

Audit Work

The Pennsylvania Department of the Auditor General conducted a performance audit of the School District of Haverford Township (SDHT). 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 SDHT in response to our prior audit recommendations.

Our audit scope covered the period March 1, 2005 through August 4, 2008, except as otherwise indicated in the audit scope, objectives, and methodology section of this report. Compliance specific to state subsidy and reimbursements was determined for school years 2005-06, 2004-05, 2003-04 and 2002-03, 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 SDHT encompasses approximately 10 square miles. According to 2000 federal census data, it serves a resident population of 48,498. According to District officials, in school year 2005-06, the SDHT provided basic educational services to 5,573 pupils through the employment of 383 teachers, 495 full-time and part-time support personnel, and 45 administrators. Lastly, the SDHT received more than \$8.9 million in state funding in school year 2005-06.

Audit Conclusion and Results

Our audit found that the SDHT complied, in all significant respects, with applicable state laws, regulations, contracts, grant requirements, and administrative procedures; however, as noted below, we identified three matters unrelated to compliance that are reported as observations.

Observation 1: Unmonitored Vendor System Access and Logical Access

Control Weaknesses. We noted the SDHT should improve controls over remote access to its computers. In particular, controls should be strengthened over outside vendor access to the student accounting applications. SDHT is in agreement in part with this observation (see page 7).

Observation 2: Internal Control Weaknesses in Administrative Policies Regarding Bus Drivers' Qualifications.

SDHT does not have written policies or procedures in place to ensure that they are notified if current bus drivers have been 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. SDHT is in agreement with this observation and has indicated that new procedures will be implemented to address the noted items (see page 12).

Observation 3: Internal Control Weakness Regarding Memorandum of Understanding.

SDHT did not review and update its Memorandum of Understanding with the local law enforcement

every two years. SDHT is in disagreement with this observation (see page 14).

Status of Prior Audit Findings and Observations. With regard to the status of our prior audit recommendations to the SDHT from an audit we conducted of the 2001-02 and 2000-01 school years, we found the SDHT had not taken appropriate corrective action in implementing our recommendations pertaining to internal control weaknesses regarding bus drivers' qualifications (see page 16).

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 March 1, 2005 through August 4, 2008, except for certification which was reviewed for the period January 12, 2005 through January 9, 2008.

Regarding state subsidy and reimbursements, our audit covered school years 2005-06, 2004-05, 2003-04 and 2002-03 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 SDHT'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 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 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 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.

SDHT 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 meeting minutes, pupil membership records, and reimbursement applications.
- Deposited state funds.

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

Lastly, to determine the status of our audit recommendations made in a prior audit report released on September 6, 2005, we reviewed the SDHT's response to DE dated December 21, 2005. We then performed additional audit procedures targeting the previously reported matters.



Findings and Observations

Observation No. 1

What is logical access control?

“Logical access” is the ability to access computers and data via remote outside connections.

“Logical access control” refers to internal control procedures used for identification, authorization, and authentication to access the computer systems.

Unmonitored Vendor System Access and Logical Access Control Weaknesses

The School District of Haverford Township uses software purchased from an outside vendor for its critical student accounting applications (membership and attendance). The software vendor has remote access into the District’s network servers.

Based on our current year procedures, we determined that a risk exists that unauthorized changes to the District’s data could occur and not be detected because the District was not able to provide supporting evidence that they are adequately monitoring vendor activity in their 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.

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.

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.

During our review, we found the District had the following weaknesses over vendor access to the District's system:

1. The District does not have evidence to support they are generating or reviewing monitoring reports of user access and activity on the system (including vendor and District employees). There is no evidence to support that the District is performing any procedures in order to determine which data the vendor may have altered or which vendor employees accessed their system.
2. The vendor uses a group userID rather than requiring that each employee has a unique userID and password.
3. The District does not require written authorization prior to the updating/upgrading of key applications or changing user data.
4. The District does not store data back-ups in a secure, off-site location.
5. The District does not have current 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.
6. The District's Acceptable Use Policy does not include provisions for privacy (e.g., monitoring of electronic mail, access to files), accountability (responsibilities of users, auditing, incident handling), and authentication (password security and syntax requirements). Further, the employees are not required to sign the policy.
7. The District has certain weaknesses in logical access controls. We noted that the District's system parameter settings do not require all users, including the vendor, to change their passwords every 30 days; to use passwords that are a minimum length of eight characters and include alpha, numeric and special characters; to maintain a password history (i.e., approximately ten passwords) and to lock out users after three unsuccessful attempts.

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

Recommendations

The *School District of Haverford Township* should:

1. Generate monitoring reports (including firewall logs) of the 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.
2. Require the vendor to assign unique userIDs and passwords to vendor employees authorized to access the District system. Further, the District should obtain a list of vendor employees with remote access to its data and ensure that changes to the data are made only by authorized vendor representatives.
3. Allow upgrades/updates to the District's system only after receipt of written authorization from appropriate District officials
4. Store back-up tapes in a secure, off-site location.
5. Establish separate IT policies and procedures for controlling the activities of vendors/consultants and have the vendor sign this policy, or the District should require the vendor to sign the District's Acceptable Use Policy.
6. Include in the District's Acceptable Use Policy provisions for privacy (e.g., monitoring of electric mail, access to files), accountability (responsibilities of users, auditing, incident handling), and authentication (password security and syntax requirements). Further, all employees should be required to sign this 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. 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 extinguishers in the computer room.

Management Response

Management agreed with our observation in part, and stated:

Haverford School District only provides remote access to our SIS [student information system] when the District is requesting technical support from our vendor. Otherwise, no remote access is possible. Once the tech support call has been resolved, this access is terminated. This is a built in procedure – outside access cannot be obtained in any other manner. We will request that our vendor provides a unique ID when accessing our system rather than a generic ID. Tech support will not alter data. Our SIS manager does all updates – tech support does not perform that function.

Haverford is in the process of revising our AUP [Acceptable Use Policy] and will require employees to sign this policy in the future.

We are reviewing our password control system as well and will be moving all District servers to another location. This should be completed by the fall of 2008. At this time we will have additional offsite back-up locations.

Haverford had requested previously to be notified by which regulation we are required to place a fire extinguisher in the server room. Our local fire department was not familiar with this regulation.

As Haverford moves forward, we would like to be advised of the policies by which we are evaluated. Is there a list of governing rules and regulations that would assist us in keeping current with such requirements? Please advise.

Auditor Conclusion

Many organizations have published numerous standards for security in IT systems. From these various publications, we have attempted to identify best practices that would prevent or detect inappropriate changes to student membership and attendance data. We do not provide Districts or other auditees with details of our audit approach in advance.

As part of a well-controlled systems development life cycle, we continue to recommend that any upgrades/updates to the District's system, by vendor or District employees, be approved in writing by the appropriate District officials.

Although there may not be specific regulations for fire safety, we continue to recommend fire extinguishers in the server room as a best practice for protecting equipment and data.

Observation No. 2 →

Internal Control Weaknesses in Administrative Policies Regarding Bus Drivers' Qualifications

Criteria relevant to the observation:

PSC Section 111 (24 P.S. § 1-111) requires prospective school employees who would have direct contact with children, including independent contractors and their employees, to submit a report of criminal history record information obtained from the Pennsylvania State Police. Section 111 lists convictions of certain criminal offenses that, if indicated on the report to have occurred within the preceding five years, would prohibit the individual from being hired.

Similarly, Section 6355 of the CPSL, 23 Pa. C.S. § 6355, requires prospective school employees to provide an official child abuse clearance statement obtained from the Pennsylvania Department of Public Welfare. The CPSL prohibits the hiring of an individual determined by a court to have committed child abuse.

The ultimate purpose of the requirements of the Public School Code and the Child Protective Services Law (CPSL) cited in the box to the left is to ensure the protection of the safety and welfare of the students transported in school buses. To that end, there are other serious crimes that districts should consider, on a case-by-case basis, in determining a prospective employee's suitability to have direct contact with children. Such crimes would include those listed in Section 111 but which were committed beyond the five-year look-back period, as well as other crimes of a serious nature that are not on the list at all. School districts should also consider reviewing the criminal history and child abuse reports for current bus drivers on a periodic basis in order to learn of incidents that may have occurred after the commencement of employment.

Our review of the personnel records of a random sample of 30 of 80 bus drivers currently employed by the School District of Haverford Township found that these individuals possessed the minimum requirements to be employed as bus drivers and that the School District of Haverford Township had on file the required report of criminal history record information and an official child abuse clearance statement for all drivers' files that we reviewed. There was no information contained in these reports that would have prohibited the School District of Haverford Township from hiring any of the drivers. Therefore, we concluded that the School District of Haverford Township has satisfied the minimum legal requirements set forth in both the Public School Code and the CPSL. Additionally, there were no serious crimes identified or other information that called into question the applicant's suitability to have direct contact with children.

However, the District does not have written policies or procedures in place to ensure that they are notified if current employees have been 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. This lack of written policies and procedures is 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.

Recommendations

The *School District of Haverford Township* should:

1. Consider developing 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 not barred by state law, affect their suitability to have direct contact with children.
2. Consider implementing 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.

Management Response

Management agreed with the observation and stated:

The District will add language to employee handbooks to encourage the disclosure of any infraction and [noting] that the District will work with the employee as much as possible.

Observation No. 3 →

Internal Control Weakness Regarding Memorandum of Understanding

Criteria relevant to this 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.

Additionally, the Basic Education Circular 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 year thereafter. (Emphasis added)

Our audit of the District's records found that the current Memorandum of Understanding (MOU) between the District and the Haverford Township Police Department was signed April 30, 2004 and has not been updated since that time.

The failure to update MOUs with all local law enforcement agencies could result in a lack of cooperation, direction, and guidance between District employees and 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.

Recommendation

The *School District of Haverford Township* should:

1. Review, update and re-execute the current MOU between itself and the Haverford Township Police Department.
2. Adopt a policy requiring the administration to review and re-execute the MOU every two years.

Management Response

Management disagreed with the observation and stated:

No information has come to my attention as Superintendent that required yearly update of the Memorandum of Understanding with the local police. This Memorandum has been self-renewing as specified in the document yearly unless otherwise amended by the parties. Since this interpretation has been brought to our attention we have started the process of updating the Memorandum of Understanding. It is currently being circulated to our District Attorney's Office and the representative assigned to the School District of Haverford Township for initial review before we meet with the local police. They also have been apprised that we are going through this process.

Auditor Conclusion

Management is correct that the Public School Code section regarding MOUs does not specifically call for periodic updates of the MOU. It is for this reason that we have addressed this in an observation rather than a finding. Our recommendation is based on our agreement with the Department of Education's Basic Education Circular and sample MOU, which implicitly suggests that MOUs be reviewed and re-executed every two years. We appreciate management's willingness to adopt the recommendations.

Status of Prior Audit Findings and Observations

Our prior audit of the School District of Haverford Township (SDHT) for the school years 2001-02 and 2000-01 resulted in one reported observation. The observation pertained to internal controls weaknesses regarding bus drivers' qualifications. As part of our current audit, we determined the status of corrective action taken by the SDHT to implement our prior recommendations. We analyzed the SDHT Board's written response provided to the Department of Education (DE), performed audit procedures, and questioned SDHT personnel regarding the prior findings. As shown below, we found that the SDHT did not implement recommendations related to the observation.

<i>School Years 2001-02 and 2000-01 Auditor General Performance Audit Report</i>		
<i>Prior Recommendations</i>	<i>Implementation Status</i>	
<p><u><i>I. Observation: Internal Control Weaknesses in Administrative Policies Regarding Bus Drivers' Qualifications</i></u></p> <ol style="list-style-type: none"> 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 not disqualifying under state law, affect their suitability to have direct contact with children. 2. Implement written policies and procedures to ensure that 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. 	<p>Background:</p> <p>SDHT did not have written policies or procedures in place to notify them if their 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.</p>	<p>Current Status:</p> <p>We followed up on the SDHT's internal control deficiencies and found that the SDHT <u>did not</u> take appropriate corrective action to improve internal controls. There is therefore another observation on this matter in our current report. (see Observation No. 2 on page 12).</p>

Distribution List

This report was initially distributed to the superintendent of the school District, the board members, our website address at www.auditorgen.state.pa.us, 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



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.

