# SHIKELLAMY SCHOOL DISTRICT

# NORTHUMBERLAND COUNTY, PENNSYLVANIA

# PERFORMANCE AUDIT REPORT

DECEMBER 2010

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

Mr. Timothy Fister, Board President
Shikellamy School District
200 Island Boulevard
Sunbury, Pennsylvania 17801

Dear Governor Rendell and Mr. Fister:

We conducted a performance audit of the Shikellamy School District (SSD) to determine its compliance with applicable state laws, regulations, contracts, grant requirements, and administrative procedures. Our audit covered the period June 23, 2006 through July 11, 2008, except as otherwise indicated in the report. Additionally, compliance specific to state subsidy and reimbursement 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 SSD complied, in all significant respects, with applicable state laws, regulations, contracts, grant requirements, and administrative procedures. 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 observations and recommendations have been discussed with SSD's management and their responses are included in the audit report. We believe the implementation of our recommendations will improve SSD's operations and facilitate compliance with legal and administrative requirements. We appreciate the SSD's cooperation during the conduct of the audit and their willingness to implement our recommendations.

Sincerely,

/s/
JACK WAGNER
Auditor General

December 23, 2010

cc: **SHIKELLAMY SCHOOL DISTRICT** Board Members

# Table of Contents

Page

Executive Summary ..... 1

Audit Scope, Objectives, and Methodology ..... 3

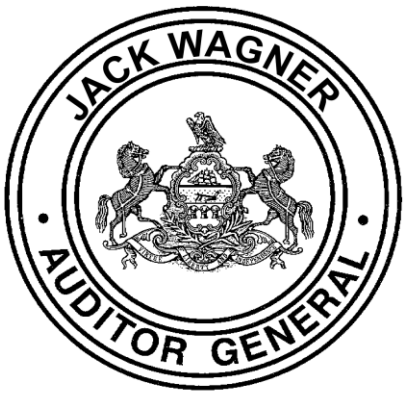
Findings and Observations ..... 6

Observation No. 1 – Unmonitored IU System Access and Logical Access Control Weaknesses ..... 6

Observation No. 2 – Memorandum of Understanding Not Updated Timely ..... 13

Status of Prior Audit Findings and Observations ..... 15

Distribution List ..... 17


JACK WAGNER
AUDITOR GENERAL

# Executive Summary

## Audit Work

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

Our audit scope covered the period June 23, 2006 through July 11, 2008, except as otherwise indicated in the audit scope, objectives and methodology section of the report. Compliance specific to state subsidy 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 SSD encompasses approximately 71 square miles. According to 2000 federal census data, it serves a resident population of 23,180. According to District officials, in school year 2005-06, the SSD provided basic educational services to 3,256 pupils through the employment of 229 teachers, 178 full-time and part-time support personnel, and 12 administrators. Lastly, the SSD received more than $15.4 million in state funding in school year 2005-06.

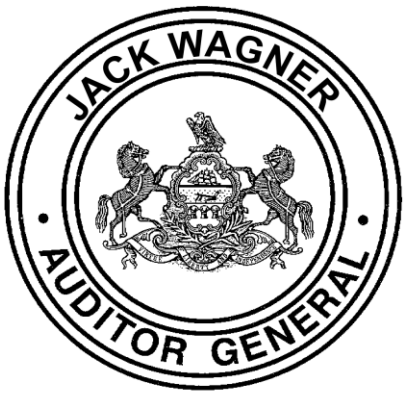
## Audit Conclusion and Results

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

**Observation 1: Unmonitored IU System Access and Logical Access Control Weaknesses**. We noted that SSD personnel should improve controls over remote access to its computers. In particular, controls should be strengthened over outside vendor access to the student accounting applications (see page 6).

**Observation 2: Memorandum of Understanding Not Updated Timely.** SSD has not updated their Memorandum of Understanding between the SSD and Sunbury Police Department since June 13, 1997 (see page 13).

**Status of Prior Audit Findings and Observations.** With regard to the status of our prior audit recommendations to the SSD from an audit we conducted of the 2002-03 and 2003-04 school years, we found the SSD had taken appropriate corrective action in implementing our recommendations pertaining to the nonpublic transportation overpayment (see page 15).


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 23, 2006 through July 11, 2008, except for the verification of professional employee certification which was performed for the period March 22, 2006 through April 24, 2008.

Regarding state subsidy and reimbursements, our audit covered school years 2004-05 and 2005-06 and 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 SSD'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 procedures. 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?
- ✓ 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 use an outside vendor to maintain its membership data and if so, are there internal controls in place related to vendor access?
- ✓ Did the District take appropriate corrective action to address recommendations made in our prior audits?

## Methodology

*What are internal controls?*

Internal controls are processes designed by management to provide reasonable assurance of achieving objectives in areas such as:

- Effectiveness and efficiency of operations;
- Relevance and reliability of operational and financial information;
- Compliance with applicable laws, regulations, contracts, grant requirements and administrative procedures.

*Government Auditing Standards* require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings, observations and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

SSD 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.
- Tuition receipts and deposited state funds.

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

Lastly, to determine the status of our audit recommendations made in a prior audit report released on December 11, 2006, we reviewed the SSD's response to DE dated February 23, 2007. We then performed additional audit procedures targeting the previously reported matters.

## Findings and Observations

**Observation No. 1**

### Unmonitored IU 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 Shikellamy School District uses software purchased from the Capital Area Intermediate Unit #15 (CAIU) for its critical student accounting applications (membership and attendance). The CAIU has remote access into the District's network servers.

Based on our current year procedures, we determined that a risk exists that unauthorized changes to the District's data could occur and not be detected because the District was unable to provide supporting evidence that they are adequately monitoring all CAIU activity in their system. However, since the District has manual compensating controls in place to verify the integrity of the membership and attendance information in its database, that risk is mitigated. Membership reconciliations are performed between manual records and reports generated from the Student Accounting System.

Reliance on manual compensating controls becomes increasingly problematic if the District would ever move into an entirely paperless future with decentralized direct entry of data into their systems. Unmonitored CAIU 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 CAIU access to the District's system:

1. The contract with the vendor did not contain a non-disclosure agreement for the District's proprietary information.

2. The contract with the vendor was not reviewed by the District's legal counsel.

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

4. The District does not have current information technology (IT) policies and procedures for controlling the activities of CAIU, nor does it require the CAIU to sign the District's Acceptable Use Policy.

5. The District does not require written authorization before adding, deleting, or changing a userID.

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

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.

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

9. The District does not have evidence to support they are generating or reviewing monitoring reports of user access and activity on the system (including CAIU and District employees). There is no evidence to support that the District is performing any procedures in order to determine which data the CAIU may have altered or which CAIU employees accessed their system.

10. The District does not maintain the servers with membership/attendance data in a restricted/secure area. The servers are located in the technology coordinator's office which is open during the normal working hours.

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

12. 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 *Shikellamy School District* should:

1. The contract with the vendor should contain a non-disclosure agreement for the District's proprietary information.

2. The contract with the vendor should be reviewed by legal counsel.

3. The District's Acceptable Use Policy should include provisions for authentication (password security and syntax requirements).

4. Establish separate IT policies and procedures for controlling the activities of vendors/consultants and have the CAIU sign this policy, or the District should require the CAIU to sign the District's Acceptable Use Policy.

5. Develop policies and procedures to require written authorization before adding, deleting, or changing a user ID.

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

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.

8. Only allow access to their system when the CAIU needs access to make pre-approved changes/updates or requested assistance. This access should be removed when the CAIU has completed its work. This procedure would also enable the monitoring of CAIU changes.

9. Generate monitoring reports (including firewall logs) of CAIU 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.

10. Maintain the servers with the membership/attendance data in a restricted/secure area in order to detect/deter unauthorized access.

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

12. 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 stated the following:

1. The contract with the vendor should contain a non-disclosure agreement for the district's proprietary information.

   Response: The Vendor has created a new contract that includes a Confidentiality Clause.

2. The contract with the vendor should be reviewed by legal counsel.

Response: Going forward, we will have the solicitor review the contract before signing. This will include the contract for the 2008-09 school year.

3. The district's Acceptable Use Policy should include provisions for authentication (password security and syntax requirements).

   Response: We will add this requirement.

4. The district should establish separate IT policies and procedures for controlling the activities of vendors/consultants and have the IU sign this policy, or the district should require the IU to sign the district's Acceptable Use Policy.

   Response: A document will be drawn up to be signed by both the district representative and the IU stating that the district will maintain access to the SIS server by allowing or disallowing PC Anywhere contact with the server. This access will be provided only when a support ticket has been issued by the district or when upgrades are needed by the IU after notification. The district will also disable the web accounts that the IU maintains until a support issue arises. The accessibility will exist until the issue has been resolved. The district will also require the IU personnel that have contact with the District SIS to sign the AUP. This will be included in the document created by the district which defines IU accessibility procedures.

5. The district should develop policies and procedures to require written authorization before adding, deleting, or changing a user ID.

   Response: We have developed a form and will use it for future hires and terminations.

6. The district should maintain documentation to evidence that terminated employees are properly removed from the system in a timely manner.

Response: We will be requiring that a form be submitted to state the date of termination for each employee that has a network account, and we will indentify on that form the date that an employee has been removed from the network and SIS.

7. The district should 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.

   Response: All personnel will be required to change their passwords in accordance with the recommendations. This will begin with the new school year.

8. The district should only allow access to their system when the IU needs access to make pre-approved changes/updates or requested assistance. This access should be removed when the IU has completed its work. This procedure would also enable the monitoring of IU changes.

   Response: The vendor is able to get into the server with PC Anywhere. It is turned off unless there is an issue whereby the vendor needs to do support for the server application. We will notify them of the need for support and will then allow access. Otherwise, the access will be turned off. We will disable their web accounts unless support is required and is mutually agreed upon.

9. The district should generate monitoring reports (including firewall logs) of IU 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.

Response: At this time, the Student Information System does not allow for this type of monitoring and logging. This will have to be addressed with the vendor. The best that can be done at this time is to restrict access to the various information, so that only those personnel that have need to modify particular records are able to do so. Attendance and grade changes are currently logged through the application.

10. The district should maintain the servers with the membership/attendance data in a restricted/secure area in order to detect/deter unauthorized access.

    Response: There is a lock on the door to the Technology Office. The servers are in a rack that is locked with a key. The servers themselves are also locked with a key to prevent a hard drive from being removed without unlocking the server. Going forward, the rack shall remain locked as will each server when authorized personnel are not in the room. The door to the room will also remain locked when authorized personnel are not in attendance, thus creating three separate locks that exist between an intruder and the data.

11. The district should develop and maintain a list of authorized individuals with access to the hardware (servers) that contains the membership/attendance data.

    Response: An authorized personnel only sign will be placed on the door. A list will be provided upon request of authorized personnel. This list will be maintained in the technology department and provided to the superintendent.

12. The district should 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.

    Response: The server room has an air conditioner to cover the requirement that servers do not get too hot. There is currently a fire detector in the room. We have requested a fire extinguisher be placed in the room.

**Observation No. 2**

## Memorandum of Understanding Not Updated Timely

*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.

Our audit of the District's records found that the current Memorandum of Understanding (MOU) between the District and the Sunbury Police Department was signed June 17, 1997 and has not been updated since.

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.

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 years thereafter. (Emphasis added)

**Recommendations**

The *Shikellamy School District* should:

1. In consultation with the solicitor, review, update and re-execute the current MOU between the District and the local law enforcement agency.

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

**Management Response**

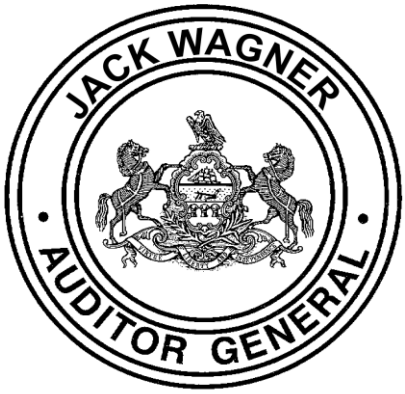
Management stated the following:

We are currently updating our school district safety procedures. We will update the MOU with our local law enforcement agencies as well as adopting a policy requiring the administration to review and re-execute the MOU on a regular basis.

## Status of Prior Audit Findings and Observations

Our prior audit of the Shikellamy School District (SSD) for the school years 2003-04 and 2002-03 resulted in one reported finding. The finding pertained to a nonpublic transportation overpayment. As part of our current audit, we determined the status of corrective action taken by the SSD to implement our prior recommendations. We analyzed the SSD Board's written response provided to the Department of Education (DE), performed audit procedures, and questioned SSD personnel regarding the prior finding. As shown below, we found that the SSD did implement recommendations related to the nonpublic transportation overpayment.

| ***School Years 2003-04 and 2002-03 Auditor General Performance Audit Report*** | | |
|---|---|---|
| ***Prior Recommendations*** | **Implementation Status** | |
| *I. Finding:* Error in Reporting the Number of Nonpublic Pupils Transported Resulted in a Net Reimbursement Overpayment of $14,245<br><br>1. Strengthen controls to ensure accurate reporting of the number of nonpublic pupils transported.<br><br>2. Thoroughly reconcile all transportation data for accuracy prior to submission of reports to DE.<br><br>3. Review reports submitted subsequent to the audit period and, if similar errors are found, submit revised reports to DE.<br><br>4. DE should adjust the District's allocations to resolve the reimbursement overpayment of $14,245. | **Background**:<br><br>Our prior audit of the District's pupil transportation reports and other financial related records for the 2003-04 and 2002-03 school years found District personnel incorrectly reported the number of nonpublic pupils transported to DE. The error resulted in a net transportation reimbursement overpayment of $14,245. | ***Current Status*:**<br><br>We followed up on the SSD nonpublic transportation reports and found that the SSD did take appropriate corrective action to improve their nonpublic transportation reporting. |


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 Thomas E. Gluck
Acting Secretary of Education
1010 Harristown Building #2
333 Market Street
Harrisburg, PA 17126

The Honorable Robert M. McCord
State Treasurer
Room 129 - Finance Building
Harrisburg, PA 17120

Ms. Barbara Nelson
Director, Bureau of Budget and Fiscal Management
Department of Education
4th Floor, 333 Market Street
Harrisburg, PA 17126

Dr. David Wazeter
Research Manager
Pennsylvania State Education Association
400 North Third Street - Box 1724
Harrisburg, PA 17105

Dr. David Davare
Director of Research Services
Pennsylvania School Boards Association
P.O. Box 2042
Mechanicsburg, PA 17055

This report is a matter of public record. Copies of this report may be obtained from the Pennsylvania Department of the Auditor General, Office of Communications, 318 Finance Building, Harrisburg, PA 17120. If you have any questions regarding this report or any other matter, you may contact the Department of the Auditor General by accessing our website at www.auditorgen.state.pa.us.