



Valentine Elementary School District

36-Month Followup of Report 21-206

The December 2021 Valentine Elementary School District performance audit found that the District did not comply with important requirements and standards, putting public monies and sensitive information at increased risk of errors and fraud and potentially risking student safety. We made **10** recommendations to the District.

District's status in implementing 10 recommendations

Implementation status	Number of recommendations
 Implemented	1 recommendation
 Not implemented	9 recommendations

The District has repeatedly failed to respond to our requests for information during our followup reviews, and its failure to cooperate during multiple followups has limited our ability to assess the District's efforts to implement the outstanding recommendations. Specifically:

- ▶ In the 18-month followup report we issued in June 2023, we were unable to report on the District's status in implementing the recommendations because it failed to provide a written response, inconsistent with its statutory responsibilities.¹
- ▶ The 24-month followup report we issued in June 2024 included multiple recommendations for which we were unable to fully evaluate the District's progress due to its lack of response to documentation requests and failure to attend multiple scheduled meetings.

¹ Arizona Revised Statutes (A.R.S.) §41-1279.03(A)(9).

- ▶ For this 36-month followup review, the District was similarly unresponsive until we notified it that we would visit the school to obtain the documentation necessary to complete this review. However, the District did not provide all requested documentation during our February 2025 District visit and did not respond to a documentation request subsequent to our visit, further limiting our review.

Given its repeated failures to respond to our requests for information and lack of progress in implementing the recommendations, we are referring this report to the Joint Legislative Audit Committee (JLAC) for its consideration and any further action. Unless otherwise directed by JLAC, this report concludes our followup work on the District's efforts to implement the recommendations from the December 2021 performance audit report.

Recommendations to the District

Finding 1: District did not comply with important requirements and standards, putting public monies and sensitive information at an increased risk of errors and fraud.

1. The District should improve controls over its purchasing process by implementing additional procedures, including requiring:

- a. An independent review of all purchase requisitions and purchase orders to ensure all have been signed by the individual requesting the purchase and by a second individual responsible for reviewing and approving the purchase before the purchase is made to demonstrate proper separation of responsibilities and prior approval.

▶ Status: **Not implemented.**

Based on our review of the District's purchases, the District continues to have issues similar to those identified during the audit and has not taken corrective action. Specifically, we judgmentally selected and reviewed 10 of 534 purchases the District made between July 2024 and January 2025 and found that 8 of the 10 purchases were made without required prior approval. Additionally, the District lacked evidence that it had implemented a secondary review process, as recommended. As a result of its inaction, the District continues to be at increased risk for unauthorized purchases.

- b. Staff review and document approval of each invoice before paying a vendor, ensuring that the purchase has been received, and billings are accurate.

▶ Status: **Not implemented.**

The District has not taken steps to address this recommendation and continues to be at risk of paying for purchases it does not receive. As discussed in recommendation 1a, we judgmentally selected and reviewed 10 of 534 purchases the District made between July 2024 and January 2025. Our review found that the District lacked documentation supporting that it had verified receiving any of the

goods or services from the 10 purchases we reviewed. The District also lacked evidence that it had verified the accuracy of the invoices associated with the purchases we reviewed prior to paying them.

2. The District should ensure staff responsible for classifying expenditures review the Uniform Chart of Accounts for school districts at least annually and any time there are revisions and updates made to it, and implement its guidance to accurately account for and report the District's spending.

► Status: **Not implemented.**

Despite District officials stating staff regularly review the Uniform System of Financial Records (USFR), we found that the District had misclassified expenditures totaling nearly \$85,000, or more than 8% of its approximately \$1,029,000 fiscal year 2025 year-to-date spending as of March 2025.² A majority of these classification errors were similar to those we identified and brought to the District's attention during the audit, including expenditures for noninstructional technology, speech language services, and conference travel. As a result of its inaction, the District continues to misreport its spending in its *Annual Financial Report*.

3. The District should improve controls over access to its Student Information System (SIS) by:

- a. Immediately removing the 6 SIS user accounts linked to terminated employees.

► Status: **Implemented at 6 months.**

- b. Developing and implementing procedures that include informing its SIS vendor in a timely manner when employees have separated from the District and verifying that the vendor has removed the terminated employees' access to reduce the risk of unauthorized access to sensitive information.

► Status: **Not implemented.**

System accounts for former District employees are not consistently and promptly disabled despite changes the District has made to its processes. As reported in our previous 24-month followup, the District developed an employee-termination checklist that includes documenting the removal of system access for former employees. Additionally, according to the District, the District's superintendent has the ability to disable user access, and District staff make efforts to complete the termination checklists and disable user access as soon as possible after staff leave the District.

However, we reviewed all 5 District employees with SIS access who separated from the District since February 2024 and found that although the District used its employee-termination checklist, the District did not consistently remove user access immediately upon employees' termination from District employment. For instance,

² The Arizona Auditor General and the Arizona Department of Education develop the USFR and related guidance pursuant to A.R.S. §15-271. The USFR and related guidance prescribe the minimum internal control policies and procedures to be used by Arizona school districts for accounting, financial reporting, budgeting, attendance reporting, and various other compliance requirements, and are in conformity with generally accepted practices and federal and State laws.

2 of the 5 employees' access was not disabled for 28 and 126 days, respectively. This time frame was substantially longer than during our previous 24-month followup where we identified 2 employees whose access was disabled within 4 and 7 days. By not immediately disabling terminated employees' access to the SIS, the District continues to increase its risk of unauthorized access to sensitive student information such as students' school, health, and other personal data.

- c. Periodically reviewing the user accounts in its SIS to determine whether all users have appropriate access levels based on their job responsibilities and, if they do not, having its vendor limit employees' access only to what the District determines is necessary to complete their job responsibilities.

► Status: **Not implemented.**

The District was unable to demonstrate that it has conducted the reviews required to address this recommendation and limit system access accordingly. According to the District, the superintendent coordinates with the District's SIS vendor to annually review SIS user accounts, and the District reported confirming with its SIS vendor that all staff have appropriate system access levels. However, the District failed to provide us with documentation of a review by either the District or the SIS vendor that specified which accounts were reviewed, how appropriate access levels were determined, and which, if any, administrator-level accounts were necessary. Additionally, as discussed in recommendation 3d, we found that the number of user accounts with administrator-level access has increased since the audit.

- d. Determining whether the number of vendor employees who have administrator-level access to its SIS is necessary and within the level of risk it is willing to accept and, if it is not, having its vendor reduce the number of employees with that access to its SIS or choosing another SIS vendor to reduce the risk of too many users with access to its sensitive student information.

► Status: **Not implemented.**

The District has not provided evidence that it has evaluated whether the number of vendor employees with administrator-level access to its SIS is necessary. Our March 2025 review of SIS administrator-level accounts found that there are 14 such accounts associated with the District's SIS vendor, which is 3 more than during the initial audit.

During our initial followup review in October 2022, the District reported that it was comfortable with the vendor's level of access and accepted any risks associated with allowing this level of access to its SIS. For this followup, the District's superintendent reported that the Board continues to support the number of accounts with access to the District's SIS.

Users with SIS administrator access can access personally identifiable information, potentially including users' social security numbers; add or delete information; and allow other users or third parties to access the system. By not ensuring that these administrator-level users require that level of access to perform their job duties, the District continues to be at an increased risk for unauthorized access to sensitive

data and potential data loss. Additionally, because hackers typically target accounts with administrator-level access for their greater access privileges, unnecessary administrator accounts can increase the likelihood of security breaches.

4. The District should review all accounting system users' access levels and work with the County to limit accounting system users' access to only those functions needed to perform their job duties.

► Status: **Not implemented.**

Our March 2025 review identified 4 accounting system users with more access than necessary to perform their job duties. Although this is fewer than the 11 users with excessive access identified in the audit, by continuing to allow excessive access to its accounting system, the District continues to increase its risk for errors, fraud, and disrupted District operations.

Finding 2: District could not demonstrate that bus drivers met all certification requirements and did not perform systematic school bus maintenance, putting student safety at risk and increasing its risk of liability

5. The District should develop and implement a procedure to track and document that its bus drivers meet all certification requirements in accordance with the State's Minimum Standards.

► Status: **Not implemented.**

The District lacks an effective process for ensuring that school bus drivers meet driver certification and testing requirements. As we reported in the initial and previous 24-month followup reports, the District continues to use a spreadsheet to track compliance with school bus driver-certification requirements. However, we found that this tracking spreadsheet is incomplete. Specifically, our February 2025 review of the District's driver-certification spreadsheet found the District did not track whether the District's school bus drivers met all certification requirements and had active fingerprint cards. For example, our review of the District's driver files found that 2 of the 4 bus drivers' Department of Public Safety certificates were not documented on the tracking spreadsheet. We also identified 1 school bus driver who lacked an up-to-date physical examination and 1 driver who was overdue for an annual drug screening.

Further, the District could not provide any evidence, either in its spreadsheet or in the driver files, that it had conducted required random alcohol testing. By not ensuring that its school bus drivers meet driver certification requirements and that it retains documentation required by the State's Minimum Standards, the District continues to increase risks to student safety.

6. The District should develop and implement procedures to track its school buses' mileage and to perform and document maintenance performance in accordance with its preventative maintenance service schedules.

► Status: **Not implemented.**

The District has not developed an effective process for tracking school buses' mileage and for ensuring that preventative maintenance services are performed when due. Our February 2025 review of the District's preventative maintenance tracking information, including bus mileage, found that it was incomplete for each of the District's 3 school buses. Additionally, we reviewed individual school bus logs and invoices for school bus maintenance services, which indicated various mechanical inspections and repairs had been performed, but these were not consistently recorded on the District's tracking system. Therefore, the District is unable to demonstrate that it is performing the required systematic maintenance on its school buses, which increases risks to student safety and may reduce school buses' useful lives.