

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, and its status in implementing the recommendations is as follows:

**Status of 10 recommendations**

Implemented	1
In process	3
<b>Not implemented</b>	<b>6</b>

We will conduct a 36-month followup with the District on the status of the recommendations that have not yet been implemented.

**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.  
**Not implemented**—Our review of a sample of 10 of the 839 purchases the District made between July 2023 and December 2023 found that the District continues to have issues similar to those identified during the audit and subsequent followup related to its purchasing procedures.<sup>1</sup> Although the 10 purchases we reviewed showed evidence of independent review and approval, 8 of the 10 purchases were made before obtaining the required prior approval. We will assess the District’s efforts to implement this recommendation at the 36-month followup.
  - b. Staff review and document approval of each invoice before paying a vendor, ensuring that the purchase has been received and billings are accurate.  
**Not implemented**—As discussed in recommendation 1a, we reviewed 10 of 839 purchases the District made between July 2023 and December 2023. Although the District indicated that an employee matches invoices to received goods and services before payment is approved, it could not provide documentation to support that the receipt of goods and services was verified prior to payment for all 10 purchases we reviewed. We will assess the District’s efforts to implement this recommendation at the 36-month followup.

<sup>1</sup> Although we published an 18-month follow-up report for Valentine ESD, the District failed to provide a response and supporting documentation necessary for our review, and we were unable to assess the implementation status for any of the recommendations at that time.

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.

**Not implemented**—Despite District officials stating they review changes to the *Uniform System of Financial Records for Arizona School Districts* (USFR) and update expenditure codes as needed, we identified misclassified expenditures of nearly \$133,000, or over 8 percent of the District's approximately \$1,567,000 fiscal year 2024 year-to-date spending as of January 2024.<sup>2</sup> Approximately half of these classification errors were similar to those that were identified during the audit, including expenditures for noninstructional technology, maintenance, construction, and speech language services. We will assess the District's efforts to implement this recommendation at the 36-month followup.

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.

**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.

**Implementation in process**—The District developed and implemented an employee termination checklist that includes documenting removing system access for employees who leave District employment. Our review of 3 District employees terminated since December 2022 found that although the District used its employee termination checklist, it took the District 4 and 7 days, respectively, to disable system access for the 2 employees who had SIS access during their District employment. Credible industry standards, such as those developed by the National Institute of Standards and Technology (NIST), indicate that access should be disabled immediately upon termination. By not immediately disabling access to the SIS for terminated employees, the District increased its risk of unauthorized access to sensitive student information such as students' school, health, and other personal data. We will assess the District's efforts to implement this recommendation at the 36-month followup.

- 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.

**Not implemented**—District officials indicated the superintendent, in coordination with the District's SIS vendor, would conduct a review of SIS user accounts in January of each year beginning in 2024. However, the District could not provide documentation that this review had occurred in January 2024 and failed to cooperate with and be present for multiple scheduled interviews with us to get additional information necessary for our follow-up work. We will assess the District's efforts to implement this recommendation at the 36-month followup.

- 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.

**Implementation in process**—District officials reported that as part of the annual review it planned to complete in January 2024, the District would require its SIS vendor to certify a list of employees with administrator-level access and the necessity for these employees to have such access in the District's SIS. The District provided a list sent from its SIS vendor in December 2023 that documented the vendor's

---

<sup>2</sup> 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.

employees with administrator-level access and an explanation for why the access was necessary. On this list, the vendor stated that each of the vendor employees were in good standing. However, the vendor's list did not clearly define what being in good standing indicated and whether it meant the employees needed administrator-level system access. Further, the District could not demonstrate that it completed its own review of the vendor's list to confirm it agreed with the vendor's assessment or reviewed other accounts not associated with vendor employees to ensure their access was appropriate. Additionally, our March 2024 review of the administrator-level access in the District's SIS system found that the vendor now has 15 accounts with administrator-level access, which is 4 more than during the audit. The District reported during the previous initial follow-up review that it was comfortable with the vendor's level of access and was willing to accept the risk associated with allowing that level of access to its SIS. We were unable to confirm if this was still accurate due to District officials failing to cooperate with and be present for multiple scheduled interviews with us to get additional information necessary to conduct our follow-up work. However, as we previously reported, by not determining whether its administrator-level users needed that level of access, the District increased its risk for security breaches, unauthorized access to and loss of sensitive data, and disruption of District operations because hackers typically target accounts with administrator-level access for their greater access privileges. We will assess the District's efforts to implement this recommendation at the 36-month followup.

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.

**Implementation in process**—Similar to the previous initial followup, our review of the District's January 2024 accounting system users' access levels found that 2 users had administrator-level access to the District's accounting system, and administrator-level access for both accounts appeared to be appropriate. Additionally, although the District has reduced the number of users with more access than necessary to perform their job duties from 6 users at the initial followup, our January 2024 review found 3 users still had more access than necessary to perform their job duties. Therefore, the District does not appear to be ensuring that employees have only the system access necessary to perform their job duties. We will assess the District's efforts to implement this recommendation at the 36-month followup.

## **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.

**Not implemented**—As we reported in the previous initial followup, the District uses a spreadsheet to track its school bus drivers' certification requirements. However, our review of the District's driver certification spreadsheet as of January 2024 found the District still did not track all certification requirements included in the State's Minimum Standards. Specifically, the District did not track the Level 1 fingerprint clearance card, the DPS bus driver certificates, or random alcohol tests, all of which the District is required to document. Our review also identified entries with errors, such as certification expiration dates in the years 1930 and 1931. Therefore, we could not determine whether all the District's school bus drivers met certification requirements. By not ensuring that its 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. We will assess the District's efforts to implement this recommendation at the 36-month followup.

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.

**Not implemented**—As we reported in the previous initial followup, the District uses a spreadsheet to track its school bus preventative maintenance. However, our review of the District's preventative maintenance spreadsheet for fiscal years 2023 and 2024 as of March 2024 found the District's procedures for tracking

and documenting school bus preventative maintenance continued to be deficient. Specifically, we reviewed preventative maintenance services performed on all 3 District school buses and found at the time of our review, 1 bus exceeded the District preventative maintenance policy's 10,000-mile interval between oil changes by at least 1,400 miles, and all 3 buses had exceeded 1 year without the annual emission service, as required by the District's school bus preventative maintenance schedule. By not demonstrating that it is performing required systematic maintenance on its school buses, the District increases risks to student safety and may lessen the school buses' useful lives due to inadequate maintenance. We will assess the District's efforts to implement this recommendation at the 36-month followup.