




Saddle Mountain Unified School District

42-Month Followup of Report 20-211

The December 2020 Saddle Mountain Unified School District performance audit found that the District's lack of compliance with important requirements and standards put public monies and sensitive information at an increased risk of errors, fraud, unauthorized access, and data loss and put student safety while being transported at risk. We made **22** recommendations to the District.

District's status in implementing 22 recommendations

Implementation status	Number of recommendations
 Implemented	12 recommendations
 Partially implemented	1 recommendation
 Not implemented	9 recommendations

In July 2023, the Joint Legislative Audit Committee (JLAC) asked the District to provide it and our Office with a plan and a reasonable timeline to implement each outstanding audit recommendation. In response, the District provided an 8-page corrective action plan to JLAC and us to address the remaining 17 recommendations it had not fully implemented at that time. Since developing its action plan, the District implemented 8 of the 17 recommendations outstanding as of July 2023 related to internal controls over its payroll process, IT administrative privileges and security awareness training, and transportation maintenance policies. The District continues to have 9 recommendations outstanding related to internal controls over purchasing, cash handling, IT system access, monitoring of adherence to key IT policies, and timely completion of school bus preventative maintenance. As noted below, our review found that the District has made some progress in implementing the outstanding recommendations but did not follow the plan it provided to JLAC in August 2023 for implementing certain recommendations. Unless otherwise directed by JLAC, this report concludes our followup work on the District's efforts to implement the recommendations from the December 2020 report.

Recommendations to the District

Finding 1: District's lack of compliance with important requirements and standards put public monies and sensitive information at an increased risk of errors, fraud, unauthorized access, and data loss

1. The District should identify and correct all overpayments made to employees.

► Status: **Partially implemented at 18 months.**

The District reviewed payments it made to employees in fiscal years 2019 (audit year) and 2020 and identified no additional overpayments. Additionally, in February 2022, the District's Governing Board voted to approve the District's response regarding its progress on the audit recommendations, which includes that the District would not correct the overpayments identified during the performance audit due to the amount of time that had passed.

2. The District should develop and implement a process to ensure employees are paid accurately by having a second employee check that the first employee entered employees' contract or hourly pay amounts accurately in the accounting system, that employees are not paid for more hours than approved on their contracts/Personnel Action Reports (PAR), and that employees' pay is accurately reduced for any unpaid leave.

► Status: **Implemented at 42 months.**

Our previous 30-month followup reported the District had developed a process for a second employee to check contract and hourly pay amounts input into the accounting system, but understaffing resulted in the District not following its new process. According to the District, it hired an additional staff member in fiscal year 2023, and it had not identified errors in pay amounts since the employee started. We judgmentally selected and reviewed 10 supplemental payroll payments, such as stipends, made to 9 of the District's 549 employees in fiscal year 2024 and found that all 10 payments were paid according to the contract or PAR and were reviewed by a second employee.

3. The District should review its purchasing policies and procedures with appropriate staff and monitor that they follow them to ensure that all purchases and payments are properly approved prior to being made.

► Status: **Not implemented.**

The District provided Uniform System of Financial Records (USFR) training for staff twice in fiscal year 2024 that included information about purchasing and cash handling, but not all employees received the training, and the District continues to lack a monitoring process to ensure its policies and procedures are followed. Specifically, District officials could not provide signed training certificates for 14 of 54 employees who, according to District officials, have cash-handling or purchasing responsibilities. Additionally, the District still lacks a formal process to monitor that its staff consistently follow purchasing policies and procedures. Our review of a judgmental sample of 8 of 4,508 fiscal year 2024 nonpayroll expenditures found that 1 purchase was made prior to being approved, 1 lacked documented approval prior to payment being made, and 1

lacked an invoice. Although the District appears to have made some efforts to address this recommendation, District staff continue to not consistently follow the District's purchasing policies, indicating that the lack of training and a formal monitoring process have likely undermined the effectiveness of the District's efforts.

Each of our 2 previous followup reports identified similar deficiencies, and although the District reported to us each time that it would take additional steps to implement this recommendation, it has not done so. Additionally, in August 2023 the District provided JLAC and us with an action plan for implementing this and other outstanding recommendations that it had developed in response to a letter from JLAC. However, despite the District's repeated assurances and the action plan it created, it has not implemented this recommendation. Therefore, unless otherwise directed by JLAC, this report concludes our followup work on the District's efforts to implement this recommendation.

4. The District should review its purchasing policies and procedures with appropriate staff and monitor that they follow them to ensure that the District pays vendors only after verifying that all purchases have been received and billings are accurate.

▶ Status: **Not implemented.**

See recommendation 3.

5. The District should review its cash-handling policies and procedures with school staff and monitor that they follow them to ensure that the District is depositing all cash collected.

▶ Status: **Not implemented.**

The District continues to have problems associated with cash handling despite reviewing its cash-handling policies and procedures and providing USFR training to school staff in August 2023 and October 2023, as discussed in recommendation 3. Our previous 30-month followup reported the District had implemented new cash-management software at 1 of its schools that the District indicated would document all cash receipts, expedite cash deposits, and ensure that all cash collected is deposited. During fiscal year 2024, the District implemented the cash-management software at its remaining 4 schools to improve cash-handling procedures.

However, our review of 35 student activities cash deposits from February 2024 for 1 school—the first to implement the cash-management software—identified multiple deficiencies. For example, 22 deposits we reviewed could not be reconciled back to the individual transactions due to a lack of documentation, and the school's financial reports for 15 of these deposits did not match the cash collected. Specifically, from each of these 15 deposits, we identified shortages of up to \$13.50 and overages of up to \$5, but the District had not performed any reconciliation to resolve the discrepancies. Additionally, there were 6 bank deposits where the bank's count of monies deposited did not match the amounts listed on deposit slips prepared by District staff. Specifically, the bank counts for 4 deposits totaled \$215.75 less cash than stated on the District's bank deposit slips, and the bank counts for 2 deposits totaled \$10 more cash than what was recorded on deposit slips. These discrepancies indicate that cash was miscounted when the deposit was prepared, or it was lost or stolen before being deposited. Finally,

contrary to the USFR, the District did not deposit cash weekly. Our review found 4 deposits that were not deposited until 8 days after cash was received.

Each of our 2 previous followup reports identified similar deficiencies, and although the District reported to us each time that it would take additional steps to implement this recommendation, it has not done so. Additionally, in August 2023, the District provided JLAC and us with an action plan for implementing this and other outstanding recommendations that it had developed in response to a letter from JLAC. However, despite the District's repeated assurances and the action plan it created, it has not implemented this recommendation. Therefore, unless otherwise directed by JLAC, this report concludes our followup work on the District's efforts to implement this recommendation.

6. The District should review its credit card policies and procedures with school staff and monitor that they follow them to ensure that staff submit all supporting documentation for credit card purchases in a timely manner so that the District can pay credit card balances on time and in full each month.

▶ Status: **Implemented at 18 months.**

7. The District should review the Uniform Chart of Accounts for school districts and implement its guidance to accurately classify all credit card transactions when reporting its spending.

▶ Status: **Implemented at 18 months.**

8. The District should limit users' access in the accounting system to only those accounting system functions needed to perform their job duties, including removing the administrator-level access from the business office employee.

▶ Status: **Implemented at 42 months.**

In the previous 30-month followup, we reported that the District had removed all inappropriate administrator-level access user accounts from the accounting system but found that 2 users still continued to have more access than necessary for their job duties, including full access to payroll. We reviewed all active users in the District's accounting system as of July 2024 and determined the District had appropriately limited users' access to the level necessary to perform their job duties.

9. The District should develop and implement a process to assign access to new users in the accounting system to ensure it is necessary for job duties.

▶ Status: **Not implemented.**

Although District officials indicated that the IT department is now responsible for assigning user roles in the accounting system, our review found that the IT department has not developed a process for assigning user roles. As explained in recommendation 8, we found that the District had limited user access to what is necessary for job duties. However, our review of the most recent revision of the District's IT policies and procedures from April 2023 determined the District still has not included a process for IT to assign user access. Having a process to assign user access ensures employees only have access to the functions needed to perform their job duties and helps ensure

appropriate separation of duties to limit the risk of unauthorized access, errors, and fraud. According to District officials, competing priorities have prevented the District from formally revising the District's IT policies and procedures to include this information. Despite the District's repeated assurances and the action plan it created (see recommendation 3), it has not implemented this recommendation. Therefore, unless otherwise directed by JLAC, this report concludes our followup work on the District's efforts to implement this recommendation.

- 10.** The District should develop and implement a process to periodically review users' access in the accounting system to ensure it is necessary for job duties.

► Status: **Not implemented.**

According to District officials, the executive director of business services reviews accounting system user access on a monthly basis. However, the District had not developed a formal process for these reviews, and the District could not provide support that these monthly reviews had been performed. Despite the District's repeated assurances and the action plan it created (see recommendation 3), it has not implemented this recommendation. Therefore, unless otherwise directed by JLAC, this report concludes our followup work on the District's efforts to implement this recommendation.

- 11.** The District should review and reduce the number of users with administrative privileges to the District's computers.

► Status: **Implemented at 42 months.**

Our July 2024 review of the District's network users with administrative privileges determined the District had removed unnecessary administrative privileges for users since the 30-month followup.

- 12.** The District should develop and implement an alternative process for staff to install and update applications that does not require local administrative privileges.

► Status: **Implemented at 42 months.**

Our previous 30-month followup reported the District had added a new server to manage and deploy Windows system and application updates to District computers so that staff do not need local administrative privileges for the updates to occur. District officials stated the new software to manage and deploy third-party application updates was installed in May 2023. The new software requires an administrator user to log in to download updates and provides automatic monthly application updates to all District computers.

- 13.** The District should review industry password standards at least annually, and implement and enforce strong network password requirements to decrease the risk of unauthorized persons gaining access to sensitive District information.

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

- 14.** The District should immediately disable or remove all network and student information system (SIS) accounts associated with terminated employees.

▶ Status: **Implemented at 18 months.**

The District has disabled or removed all network and SIS accounts associated with terminated employees that were identified during the audit.

- 15.** The District should develop and implement a process to ensure that terminated employees have their network and SIS access promptly removed to reduce the risk of unauthorized access.

▶ Status: **Not implemented.**

Our previous 30-month followup reported the District had added network and SIS access removal to its employee-separation checklist. However, our July 2024 review of all active accounts in the District's network and our October 2024 review of all active accounts in the SIS network found 2 network accounts associated with terminated employees, only 1 of which had the required separation checklist completed. Additionally, our review found 1 SIS account that was not removed until nearly 2 months after the employee no longer worked for the District and 1 network account that was not removed until nearly 3 months after the employee no longer worked for the District. By not immediately removing network and SIS access for terminated employees, the District increased the risk of unauthorized access to its critical IT systems and potential data loss. Despite the District's repeated assurances and the action plan it created (see recommendation 3), it has not implemented this recommendation. Therefore, unless otherwise directed by JLAC, this report concludes our followup work on the District's efforts to implement this recommendation.

- 16.** The District should require all employees to participate in a security awareness training if they have not done so in the past year.

▶ Status: **Not implemented.**

According to District officials, since the 30-month followup, the District added security awareness training to the mandatory annual training provided through a digital platform. However, we found that not all employees completed the training as required. Our review of 100 of the District's 549 employees in fiscal year 2024 identified 45 employees who did not complete the required security awareness training module, indicating the District is not monitoring staff to ensure its policy is being followed. District officials explained that employees hired after the start of the year were not informed of the training and that some just did not take the training. We have identified similar issues in the 2 previous followups, and despite the District's repeated assurances and the action plan it created (see recommendation 3), it has not implemented this recommendation. Therefore, unless otherwise directed by JLAC, this report concludes our follow-up work on the District's efforts to implement this recommendation.

- 17.** The District should establish and implement a District policy to conduct security awareness training on a regular basis, at least annually.

► Status: **Implemented at 42 months.**

Our previous 30-month followup reported the District had established a policy in April 2023 to conduct annual security awareness training but was still in the process of developing the training content. The District has since developed the training and utilized it in fiscal year 2024.

- 18.** The District should review its IT contingency plan to ensure it is complete; test its plan at least annually to identify and remedy any deficiencies, which should include testing the District's ability to restore electronic data files for critical systems from backups; and document the test results.

► Status: **Not implemented.**

Our previous 30-month followup reported that although the District had reviewed and updated its IT contingency plan, the plan was still missing a plan for business continuity and some information from the detailed restoration steps, such as system and configuration hardware requirements and the location of backups. The District has not substantially revised the contingency plan since the previous 30-month followup, and although the District had an additional Disaster Recovery Plan, that plan did not address the missing components identified in our previous 30-month followup report. Additionally, District officials reported they tested the loss of internet using Wi-Fi hotspots but could not provide documentation to support having conducted such a test or the results of the test. The District indicated that it did not complete a test of the full contingency plan, contrary to requirements. Despite the District's repeated assurances and the action plan it created (see recommendation 3), it has not implemented this recommendation. Therefore, unless otherwise directed by JLAC, this report concludes our followup work on the District's efforts to implement this recommendation.

Finding 2: District did not timely maintain school buses and sometimes transported students in unallowable vans, putting student safety at risk

- 19.** The District should develop and implement a formal preventative maintenance policy that stipulates the number of miles a bus can travel or the amount of time that can elapse before a bus will receive preventative maintenance.

► Status: **Implemented at 42 months.**

Since the initial audit, the District has developed and implemented a formal preventative maintenance policy that stipulates the number of miles a school bus can travel or the amount of time that can elapse before a school bus should receive preventative maintenance. The District's policy also requires a preventative maintenance inspection checklist be completed each time the school bus is brought in for maintenance. The District now includes the preventative maintenance inspection checklist in its documentation retained for school bus preventative maintenance.

- 20.** The District should revise its process for tracking when buses are due for preventative maintenance and ensure that required preventative maintenance is identified and completed

in accordance with the State's Minimum Standards and the District's formal preventative maintenance policy.

► Status: **Not implemented.**

Our previous 30-month followup reported the District had programmed the vehicle engines to track mileage and alert drivers when maintenance is due, and as mentioned in recommendation 19, the District developed a formal preventative maintenance policy. However, our review of preventative maintenance checklists for a judgmentally selected sample of 5 of the District's 29 school buses in fiscal year 2024 found that the District was not completing preventative maintenance in accordance with its policy and not properly documenting maintenance when it was performed. Specifically, 2 of 10 recorded oil changes we reviewed were not completed within the mileage stipulated by the District's policy. We could not determine whether 2 different oil changes we reviewed complied with the District's policy because the District's records lacked recorded mileage on the preventative maintenance forms. Further, most of the preventative maintenance checklists we reviewed were incomplete, including missing required school bus mileage and school bus number recordings that are necessary for the District to demonstrate it performed the appropriate maintenance within the required interval. Although the District has established a new preventative maintenance policy since the initial audit, it does not consistently complete and document preventative maintenance in accordance with its policy or monitor staff's completion of these documents, potentially increasing risks to student safety and reducing its school buses' useful lives. Despite the District's repeated assurances and the action plan it created (see recommendation 3), it has not implemented this recommendation. Therefore, unless otherwise directed by JLAC, this report concludes our followup work on the District's efforts to implement this recommendation.

21. The District should stop using its 12- and 15-passenger vans for student transportation.

► Status: **Implemented at 42 months.**

According to District officials, the District no longer transports students in 12- and 15-passenger vans.

22. The District should identify and implement ways to transport all students using vehicles that meet all required safety standards, such as developing a list of substitute certified bus drivers so that the District can transport all students in its school buses.

► Status: **Implemented at 42 months.**

As discussed in recommendation 21, District officials indicated that the District no longer transports students in 12- and 15-passenger vans. Additionally, District officials indicated that after increasing wages, the District now has sufficient certified school bus drivers to transport all students in its school buses.