ARIZONA Auditor General
Making a Positive Difference

Heber-Overgaard Unified School District

24-Month Followup of Performance Audit Report 23-210

The December 2023 Heber-Overgaard Unified School District performance audit found that the District had lower spending in most operational areas, but lacked some required internal controls and did not comply with important IT security requirements, putting public monies and sensitive computerized data at risk. The CPA firm Walker & Armstrong, who conducted the audit under contract with the Arizona Auditor General, made **21** recommendations to the District. In addition to reporting on the status of the District's efforts to implement these recommendations, we have also provided an update at the end of this followup on the District's compliance status with the *Uniform System of Financial Records for Arizona School Districts* (USFR).[1]

District's status in implementing 21 recommendations

Implementation status	Number of recommendations
✓ Implemented	13 recommendations
– Partially implemented	8 recommendations

Unless otherwise directed by the Joint Legislative Audit Committee, this report concludes our followup work on the District's efforts to implement the recommendations from the December 2023 report.

[1] The Arizona Auditor General and the Arizona Department of Education jointly developed the USFR pursuant to Arizona Revised Statutes (A.R.S.) §15-271. The USFR and related guidance prescribes 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.

Recommendations to the District

Finding 1: District lacked important internal controls, putting public monies at an increased risk for unauthorized purchases and fraud and potentially compromising student safety and sensitive personnel information

1. The District should develop and implement procedures to ensure the District obtains and documents appropriate approvals in advance of making purchases, as required by the USFR and District policy.

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

  The District developed and adopted new purchasing policies and procedures, which include ensuring appropriate approvals are obtained in advance of making purchases and consequences for unauthorized purchases such as personal liability for unauthorized purchases, suspension, or termination. We judgmentally selected and reviewed 4 of 36 fiscal year 2024 travel expenditures to determine whether the District consistently followed the new procedures. Our review found that all 4 expenditures had documented prior approval, in accordance with the District's updated procedures.

2. The District should develop and implement procedures to ensure employees and board members complete conflict-of-interest disclosure forms upon hire or the beginning of their term and annually thereafter in accordance with District policy.

- Status: **Partially implemented at 24 months.**

  The District implemented procedures to ensure that all District employees and Board members complete conflict-of-interest disclosure forms upon hire or at the beginning of their term and annually thereafter. We requested the District's fiscal year 2026 disclosure forms for all 5 Board members and 11 administrative employees and found that the District had current forms on file for all 16 individuals. However, some of the 16 forms were incomplete. Specifically, despite the District's conflict-of-interest forms requiring the person reporting a substantial interest to describe the substantial interest, 5 employees who disclosed substantial interests on their disclosure forms did not provide key details related to their conflicts such as their title, role, responsibilities, relationship, or compensation associated with the substantial interests they disclosed. Ensuring conflicts are fully disclosed is important to ensure conflicts are appropriately identified, communicated, and remediated.

3. The District should review completed conflict-of-interest disclosure forms timely to identify and communicate conflicts of interest to the appropriate personnel to ensure the District takes action to remediate disclosed conflicts of interest to comply with District policies and State conflict-of-interest laws.

- Status: **Partially implemented at 24 months.**

The District has developed a process that requires administrative staff to review employees' and Board members' conflict-of-interest disclosure forms for completeness before the superintendent's review to determine any actions necessary to remediate disclosed conflicts. However, as explained in recommendation 2, we identified 5 fiscal year 2026 disclosure forms that were incomplete because they did not include key details about disclosed substantial interests, which indicates the District has not consistently followed its process for reviewing completed disclosure forms. Additionally, 3 of the 5 incomplete disclosure forms lacked evidence of administrative staff and/or the superintendent's review, contrary to the District's process. District officials indicated that, based on their personal knowledge, they were aware of these conflicts and would ensure these employees refrained from participating in matters related to their conflicts of interest, despite their incomplete forms. However, incomplete forms increase the risk the District may miss or be unaware of substantial interests it must act to remediate and does not provide the public with statutorily required information about disclosed conflicts.[2]

4. The District should develop and implement a process to ensure that all required personnel have a valid fingerprint clearance card, including:

a. Maintaining documentation to support that all employees have fingerprint clearance cards if they are statutorily required to have one.

- Status: **Implemented at 24 months.**

  The District developed and implemented a process to maintain documentation to support that all employees have fingerprint clearance cards if they are statutorily required to have one. We judgmentally selected and reviewed fingerprint clearance cards for 7 current and former District employees and found that the District had documentation to support that all 7 employees had valid fingerprint clearance cards.

b. Monitoring and regularly reviewing employees' fingerprint clearance cards to confirm their validity.

- Status: **Partially implemented at 24 months.**

  The District maintains a list of employee fingerprint clearance cards that includes employee names, issuance dates, and expiration dates, and District officials indicated they review this list twice annually to identify and renew expiring fingerprint clearance cards. We reviewed the District's list and compared it to the 7 employee fingerprint clearance cards we reviewed and found that the employee records on the District's list were accurate. Additionally, we found that the District's list had evidence of review in February 2026, including identifying upcoming expirations. However, the District's February 2026 review only identified expiring fingerprint clearance cards and did not include a process for confirming the validity of employees' fingerprint clearance cards by reviewing the Arizona Department of Public Safety's (DPS)

[2] A.R.S. §38-509 requires political subdivisions, including school districts, to maintain for public inspection a special file that includes all documents necessary to memorialize all substantial interest disclosures.

website. Regularly confirming the validity of fingerprint clearance cards is important because DPS may suspend/revoke the card if a cardholder is arrested/convicted of a precluding offense. The District indicated it plans to implement procedures to verify fingerprint clearance cards' validity twice yearly through the DPS website and provide employee training on its updated procedures by August 2026.

5. The District should secure and retain personnel files in accordance with applicable document retention schedules.

- Status: **Implemented at 24 months.**

  We judgmentally selected and reviewed 7 current and former District employee personnel files to determine if the District had retained files in accordance with records retention requirements and found that the District had appropriately retained files for all 7 employees we reviewed.

6. The District should develop and implement a process for appropriately providing personnel records to terminated employees and require training for responsible employees regarding the process.

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

  Since the audit, the District developed and implemented a policy for providing personnel records to terminated employees. Additionally, the District provided training for responsible employees regarding the process for providing personnel records.

7. The District should develop and implement policies and procedures for monitoring and reviewing usage logs for all District vehicles that includes ensuring vehicles are only used for an authorized purpose.

- Status: **Partially implemented at 24 months.**

  In February 2026, the District adopted policies and procedures for District vehicle use, including that vehicles may only be used for authorized District business. The District's updated procedures specify requirements related to completing and submitting usage logs with information including date of use, mileage, destination, and the travel's purpose. Additionally, to further monitor usage of its 40 vehicles, the District installed GPS tracking devices on 12 of its most frequently used vehicles. However, the District's updated procedures do not specify requirements related to reviewing vehicle usage records to ensure vehicles are being used only for authorized District purposes. We reviewed usage logs from December 2025 for 5 of the District's vehicles and found that the logs documented the required information, but only 1 usage log showed evidence that the transportation director had reviewed it. The District's transportation director indicated having reviewed the other 4 usage logs but stated they lacked a process to document their review. Conducting and documenting reviews of vehicle usage logs is important to ensure vehicles are used only for authorized purposes and any usage contrary to the District's policy is appropriately and timely addressed.

Finding 2: Districts excessive access to sensitive computerized data and other IT deficiencies increased the risk of unauthorized access to sensitive information, errors, fraud, and data loss

8. The District should implement and enforce strong password requirements that align with credible industry standards to decrease the risk of unauthorized persons gaining access to sensitive District information and disrupting operations.

- Status: **Implemented at 24 months.**

  Our March 2026 review found that the District enforced strong password requirements that align with credible industry standards.

9. The District should develop and implement policies and procedures to review the District's password standards against industry password standards at least annually.

- Status: **Partially implemented at 24 months.**

  In March 2026, the District updated its password security policies and procedures to require an annual review of the District's password standards against credible industry standards. The District reported that it plans to have this updated policy approved by its Board and complete a review of its password standards by May 2026.

10. The District should protect its sensitive computerized data by limiting users' access in the accounting system to only those accounting system functions needed to perform their job duties, including removing business office employee's administrator-level access.

- Status: **Partially implemented at 24 months.**

  As we reported in the prior initial followup, our August 2024 review found that the District had removed business office employees' administrator-level access in the accounting system. Our March 2026 review of users' access levels for all 20 active users in the District's accounting system found that the District continued to appropriately limit administrator-level access to nonbusiness office employees.

  However, 9 District users continued to have more system access than needed to perform their job duties and could initiate and complete purchasing and/or payroll transactions without an independent review and approval. The District indicated it had implemented some compensating controls to reduce the risk of excessive system access, such as only authorizing certain users to provide vouchers to the County for processing. However, the compensating controls the District described were insufficient to address risks of excessive system access for all 9 users we identified. By continuing to allow excessive access to its system, the District increases the risk of errors and fraud.

11. The District should develop and implement written policies and procedures to assign and periodically review accounting system access for employee accounts to ensure they have access to only those accounting system functions needed to perform their job duties. If separation of duties is not feasible due to a limited number of personnel, the District should implement other controls such as a process for a supervisor to regularly review system logs, balancing reports, and other relevant indicators, as required by the USFR.

- Status: **Partially implemented at 24 months.**

  In October 2025, the District updated its IT policies and procedures to include guidance for assigning and periodically reviewing accounting system user access. The procedures indicate that accounting system access is to be assigned such that users should have access only to the functions necessary to perform their job duties. Additionally, the procedures require the District to review all user accounts at least twice each year to ensure access is necessary and appropriate. In January 2026, the District completed and documented its review of accounting system user access. The District's review determined that accounting system access appeared appropriate. However, as previously discussed in recommendation 10, we identified 9 users who had more access than needed to perform their job duties and could initiate and complete purchasing and/or payroll transactions without an independent review and approval, indicating that the District's review process was insufficient and may need to be updated.

12. The District should immediately disable or remove all network accounts associated with terminated employees.

- Status: **Implemented at 24 months.**

  Our January 2026 review of the District's network found that the District disabled or removed all network accounts associated with terminated employees.

13. The District should evaluate and document whether terminated employees accessed the District's network after their employment ended, such as unauthorized activities or changes that may have occurred as a result of potential improper access and remedy any identified effects.

- Status: **Implemented at 24 months.**

  In July 2025, the District completed a review to determine whether terminated employees improperly accessed the District's network after their employment ended and determined that none had done so. We randomly selected 2 employees whose District employment terminated in fiscal year 2025 and found that the District promptly removed these employees' access upon termination and documented the date of access removal or password reset. Additionally, as discussed in recommendation 12, we found that the District had removed all network accounts associated with terminated employees.

14. The District should establish written policies and procedures to ensure that terminated employees' network access is promptly removed.

- Status: **Implemented at 24 months.**

  In October 2025, the District updated its IT policies and procedures to ensure terminated employees' network access is promptly removed. Additionally, as explained in recommendation 12, our January 2026 review found that the District disabled or removed all network accounts associated with terminated employees.

15. The District should develop and implement an IT contingency plan that meets USFR requirements and credible industry standards and test the plan at least annually to identify and remedy any deficiencies and document the test results.

- Status: **Implemented at 24 months.**

  In November 2025, the District updated and approved an IT contingency plan that meets USFR requirements and credible industry standards. In December 2025, the District tested its plan and documented the results in accordance with its policy, which requires the District to test the plan annually.

16. The District should restrict physical access to its IT server room so that only appropriate personnel have access.

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

  We reviewed the District's IT server room key inventory list and key agreements and confirmed that the District had restricted access to its IT server room to a limited number of appropriate personnel. Additionally, the District installed security cameras in the IT server room as an additional control to monitor access.

17. The District should develop and implement a written policy for distributing, tracking, and collecting keys that requires employees to sign an agreement outlining their responsibilities and that would allow the District to account for all keys.

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

  We reviewed the District's key policy, which outlines requirements including logging key assignments, returning keys, reporting lost keys, and completing key agreements. We also reviewed the District's key agreements, which are required to be completed by each individual assigned a key and include information about each key assigned, such as areas of access and date issued and returned, and outline applicable rules and consequences for loss or misuse. As discussed in recommendation 16, we reviewed the District's key agreements for IT server room access and found that all employees had appropriately completed the District's key agreement. Further, we found that the District maintained an inventory of all IT server room key assignments to allow it to account for all keys and ensure keys are returned upon termination, as discussed in recommendation 18.

18. The District should conduct a physical inventory to determine and document the number of keys that exist and who has access to IT areas.

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

  The District conducted a review and identified the number of existing keys for IT areas. The District accounts for and documents all assigned keys that access IT areas on a key inventory list and stores unassigned keys in a locked location. District officials stated that when an employee returns a key, the District's receipt of the key is documented on the inventory list, and the key is stored in a secure location. Additionally, the District has a process for reconciling its key inventory to ensure assigned and unassigned keys are accounted for. As discussed in recommendations 15 and 16, we reviewed the District's IT key inventory list and key agreements and found that the District has documented key assignments and who has access to their IT areas, and the District has installed security cameras to further monitor who has access to these areas. Additionally, we reviewed key assignments for 2 terminated employees and determined that the District collected the keys assigned to both employees promptly upon termination. Finally, our review of the District's unassigned keys found that the District had accounted for all keys it identified during its review that access IT areas and had stored unassigned keys in a secure location.

19. The District should perform regular inspections of IT areas for maintenance needs to protect property and data.

- Status: **Implemented at 24 months.**

  In October 2025, the District updated and implemented procedures to perform and document semiannual inspections of IT areas for maintenance needs that include checking ceiling tiles for water damage, which was a concern identified during the performance audit. In January 2026, the District performed and documented 2 inspections of IT areas and did not identify any concerns.

20. The District should develop comprehensive IT security policies and procedures in alignment with USFR requirements, and ensure they are consistently communicated to and implemented by staff to address the identified deficiencies and discrepancies in current operations.

- Status: **Partially implemented at 24 months.**

  The District worked with an IT cyber security vendor to update and implement comprehensive IT security policies and procedures that align with USFR requirements and that address most of the deficiencies identified during the performance audit (see recommendations 8 through 19). However, some deficiencies persist because, as discussed in recommendation 10, the District continued to allow excessive system access for some accounting system users.

District USFR noncompliance

District is no longer in noncompliance with the USFR as of April 2026 based on our review of the District's fiscal year 2025 financial audit reports and USFR Compliance Questionnaire (Questionnaire), and fiscal years 2025 and 2026 records and procedures

Prior to April 2026, Heber-Overgaard Unified School District had been in noncompliance with the USFR since August 2025. On April 17, 2026, we sent a letter to the District notifying it that we had reviewed the District's fiscal years 2025 and 2026 records and procedures as of January 2026 and received the District's fiscal year 2025 financial audit reports and Questionnaire. Based on our review of all available information at that time, including the number and significance of the District's outstanding deficiencies, we determined that the District was no longer in noncompliance with the USFR. However, as noted in our April 2026 letter, the District continues to have some outstanding procurement deficiencies and it has not fully implemented certain recommendations described in this followup related to conflicts of interest, vehicle usage, and IT controls. The District must act to correct the outstanding deficiencies to ensure continued compliance with USFR requirements.