




Heber-Overgaard Unified School District

Initial Followup of 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.

District's status in implementing 21 recommendations

Implementation status		Number of recommendations
	Implemented	5 recommendations
	In process	5 recommendations
	Not implemented	11 recommendations

We will conduct a 24-month followup with the District on the status of the recommendations that have not yet been implemented.

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: **Implementation in process.**

District officials stated that their procedures require all full-time employees to complete conflict-of-interest disclosure forms at the beginning of each school year during staff training. Additionally, Board members must complete the form twice per year, in July and December, to ensure that all Board members complete it at least annually. We requested the District's fiscal year 2025 conflict-of-interest disclosure forms for all 5 Board members and all 8 administrative employees. We found that the District had forms on file for all 13 individuals, and all forms were completed at the beginning of the fiscal year, consistent with the District's procedures. However, we identified forms that were missing required information or had been completed inaccurately. Specifically, despite the District's conflict-of-interest forms requiring the person reporting a substantial interest to describe the substantial interest, 2 employees who disclosed substantial interests on their disclosure forms did not provide enough information to fully disclose their conflicts. These 2 employees failed to include details such as their title, role, responsibilities, relationship, or compensation associated with the substantial interests they disclosed. Additionally, 1 of these and another employee who disclosed conflicts of interest on their forms erroneously signed the statement of no conflict on their form, attesting they did not have a conflict to disclose. Instead, the 2 individuals should have signed the statement of disqualification attesting that they will refrain from participating in any manner in the conflicts disclosed, but failed to do so. We will assess the District's efforts to implement this recommendation at the 24-month followup.

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: **Implementation in process.**

The District reported that 2 administrative employees review all completed conflict-of-interest disclosure forms when employees and/or Board members submit them. If their review identifies a disclosed conflict-of-interest, the superintendent also reviews the form and discusses disclosed conflicts with the individual who completed the form as needed to ensure the superintendent fully understands the conflict. We reviewed 13 fiscal year 2025 conflict-of-interest disclosure forms—8 employee forms and 5 Board member forms—and found that the superintendent had reviewed all disclosed conflicts. However, none of the forms had evidence that the 2 administrative employees had reviewed them. Additionally, although the superintendent disclosed conflicts on their disclosure form and self-reviewed the form, there was no evidence of an independent review by another individual, such as a Board member. Further, as discussed previously, some of the District's disclosure forms were inaccurate and/or incomplete, which the District did not identify during its review of the disclosure forms and could impact the District's ability to appropriately identify, communicate, and remediate potential conflicts. We will assess the District's efforts to implement this recommendation at the 24-month followup.

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: **Not implemented.**

We judgmentally selected and reviewed fingerprint clearance cards for 13 District employees and found that the District had valid fingerprint clearance cards for 10 of these employees. Two employees were new to the District and had applied for fingerprint clearance cards but had not yet received them, and therefore the District did not have the cards on file. Additionally, we found that the District did not have an up-to-date fingerprint clearance card for 1 employee we reviewed. We will assess the District's efforts to implement this recommendation at the 24-month followup.

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

► Status: **Not implemented.**

The District stated it maintains a list of employee fingerprint clearance cards that includes employee names, issuance dates, and expiration dates and that they review this list at least twice annually to confirm the validity of each employee's card. However, we compared the District's list to the 13 employee fingerprint clearance cards we reviewed and found that 9 employee records on the District's list were

inaccurate. Specifically, 3 employees were not included on the list, and 6 employee records had incorrect card expiration dates. The District provided valid fingerprint clearance cards for the 6 employees with incorrect card expiration dates, as well as evidence of fingerprinting submission for the 2 new employees previously discussed. However, the District could not provide an updated fingerprint clearance card for 1 employee. By not ensuring all employees have valid fingerprint clearance cards as required, the District continues to increase potential risks to students. We will assess the District's efforts to implement this recommendation at the 24-month followup.

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

► Status: **Not implemented.**

We reviewed a sample of 5 current and former District employee personnel files to determine if the District had retained the files in accordance with records retention requirements and found that District had not appropriately retained files for all 5 employees we reviewed.¹ Specifically, 1 current employee's file did not contain the required background investigation. District officials stated that due to staff turnover, they failed to obtain the file from a former administrator prior to the administrator's termination. District officials further stated they have implemented a process to prevent similar errors in the future. Additionally, as discussed previously in recommendation 4a, we found that 1 employee's file did not have an updated fingerprint clearance card, and therefore, the District had not retained the required documentation in accordance with applicable personnel file requirements. We will assess the District's efforts to implement this recommendation at the 24-month followup.

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: **Not implemented.**

District officials indicated that they track mileage on all District vehicles and instruct employees on properly completing usage logs. Additionally, they stated that the transportation director reviews usage logs each month to verify their accuracy and completeness. However, our review of 6 months of fiscal year 2024 usage logs for 5

¹ The Arizona State Library and Archives' records retention schedules indicate that personnel records should be maintained for 5 years after an employee's termination.

of the District's 20 vehicles identified several errors that the transportation director's reviews had not identified or addressed. Specifically, for 1 vehicle's usage log we reviewed, the same beginning odometer readings were recorded for multiple trips. Further, we found that for 2 other vehicles, District staff traveled more than 1,900 miles but had not documented the purpose of the travel on the vehicle's usage logs. The District's procedures for tracking, monitoring, and reviewing usage logs appear to be ineffective for accurately recording mileage and ensuring that vehicles are only used for an authorized purpose. We will assess the District's efforts to implement this recommendation at the 24-month followup.

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: **Implementation in process.**

At the time of our review in August 2024, the District required multifactor authentication for users to sign into District computers and servers. However, our review of the District's network password requirements found that the District had not updated its network password requirements to be consistent with credible industry standards. Additionally, District officials stated that the District had an informal policy to change passwords for shared network accounts when users with access left District employment but stated it did not follow this practice. By having password requirements that do not meet credible industry standards and not enforcing its policy to change passwords on shared network accounts, the District increases the risk for unauthorized access to its systems and sensitive data. We will assess the District's efforts to implement this recommendation at the 24-month followup.

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: **Not implemented.**

The District has not developed and implemented policies and procedures to review the District's password standards against credible industry password standards at least annually. The District reported it will develop and implement such policies and procedures by the end of May 2025 as part of the comprehensive IT security policies and procedures it is currently developing. We will assess the District's efforts to implement this recommendation at the 24-month followup.

- 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: **Implementation in process.**

Our August 2024 review of users' access levels for all 17 active users in the District's accounting system found that the District removed business office employees' administrator-level access. However, 9 District users continued to have 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. By continuing to allow excessive access to its systems, the District increases the risk of errors and fraud. We will assess the District's efforts to implement this recommendation at the 24-month followup.

- 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: **Not implemented.**

The District has not developed and implemented policies and procedures to assign and periodically review system access for employee accounts. The District reported it will develop and implement such policies and procedures by the end of May 2025 as part of the comprehensive IT security policies and procedures it is developing. We will assess the District's efforts to implement this recommendation at the 24-month followup.

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

► Status: **Implementation in process.**

Our August 2024 review of the District's network found that the District disabled the 10 network accounts associated with terminated employees that were identified in the initial audit. However, we found the District was still not immediately disabling accounts when no longer needed, as we identified 1 active network user account associated with a terminated employee. The account we identified was associated with a District employee who had not been employed by the District for approximately 1 month prior to our review. When we brought this account to the District's attention during the followup, the District reported it terminated its system access and that it was an oversight that the account had not been disabled or removed. We will assess the District's efforts to implement this recommendation at the 24-month followup.

- 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: **Not implemented.**

The District has not completed a review of whether terminated employees improperly accessed the District's network after their employment ended. The District's process for removing access makes it such that they likely cannot distinguish whether it was the terminated employee or IT personnel who accessed the account after the terminated employee left District employment. Specifically, District officials stated that the District's IT department resets employees' network and multifactor authentication passwords when an employee leaves District employment since other District employees may need access to data and files on the terminated employee's computer after they are no longer employed by the District. However, we found that District IT staff do not always remove terminated employees' access on the same day the employee is terminated and do not always document the date of the password reset.

District officials indicated they could not find documentation for the 11 network accounts associated with terminated employees discussed in recommendation 12 and therefore had no record of the date of access removal or password reset for these accounts. Absent this documentation, the District will likely be unable to assess whether these employees improperly accessed the District's network after their employment ended and remedy any identified effects. Therefore, the District should ensure it removes terminated employees' access immediately upon termination and documents the date of access removal and password reset for all accounts. We will assess the District's efforts to implement this recommendation at the 24-month followup.

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

► Status: **Not implemented.**

The District has not established written policies and procedures to ensure that terminated employees' network access is promptly removed. The District reported it will develop and implement such policies and procedures by the end of May 2025 as part of the comprehensive IT security policies and procedures it is developing. We will assess the District's efforts to implement this recommendation at the 24-month followup.

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: **Not implemented.**

Our February 2025 review of the District's IT contingency plan found that the plan was incomplete and was missing key components recommended by credible industry standards. Specifically, the plan did not identify all critical systems and the order in which they should be restored, and did not include individual responsibilities during a disaster, plans for business continuity, or detailed restoration steps. Additionally, the

plan was not reviewed and approved by appropriate District staff. We will assess the District's efforts to implement this recommendation at the 24-month followup.

- 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 the 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: **Not implemented.**

Although the District's IT Director reported performing informal inspections when performing work in the District's IT server rooms, the District does not have inspection policies or procedures or a process for regular inspections of IT areas. The District reported it will develop and implement such policies and procedures by the end of May 2025 as part of the comprehensive IT security policies and procedures it is developing. We will assess the District's efforts to implement this recommendation at the 24-month followup.

- 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: **Not implemented.**

The District has not developed comprehensive IT security policies and procedures in alignment with USFR requirements. The District reported it is working with an IT cybersecurity vendor to develop a comprehensive IT security policy and procedure manual and expects the manual to be completed by the end of May 2025. We will assess the District's efforts to implement this recommendation at the 24-month followup.