



LINDSEY A. PERRY
AUDITOR GENERAL

ARIZONA
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

December 29, 2023

Members of the Arizona Legislature

The Honorable Katie Hobbs, Governor

Governing Board
Heber-Overgaard Unified School District

Mr. Ron Tenney, Superintendent
Heber-Overgaard Unified School District

Transmitted herewith is a report of the Auditor General, *A Performance Audit of Heber-Overgaard Unified School District*, conducted pursuant to Arizona Revised Statutes §41-1279.03. I am also transmitting within this report a copy of the Report Highlights to provide a quick summary for your convenience. The CPA firm Walker & Armstrong conducted this performance audit under contract with the Arizona Auditor General.

This school district performance audit assessed the districts' spending on noninstructional areas, including administration, student transportation, food service, and plant operations, and made recommendations to the District to maximize resources available for instruction or other District priorities. As outlined in its response, the District agrees with all the findings and recommendations and plans to implement all the recommendations. My Office will follow up with the District in 6 months to assess its progress in implementing the recommendations. I express my appreciation to Superintendent Tenney and District staff for their cooperation and assistance throughout the audit.

My staff and I will be pleased to discuss or clarify items in the report.

Sincerely,

Lindsey A. Perry

Lindsey A. Perry, CPA, CFE
Auditor General

Heber-Overgaard Unified School District

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



Walker & Armstrong

CERTIFIED PUBLIC ACCOUNTANTS AND ADVISORS

December 27, 2023

Lindsey A. Perry, CPA, CFE
Arizona Auditor General
2910 North 44th Street, Suite 410
Phoenix, Arizona 85018

Dear Ms. Perry:

We are pleased to submit our report in connection with our performance audit of Heber-Overgaard Unified School District for fiscal years 2022 and 2023, conducted pursuant to Arizona Revised Statutes §41-1279.03.

As outlined in its response, the District agrees with the findings and recommendations and plans to implement all the recommendations.

We appreciate the opportunity to provide these services and work with your Office. Please let us know if you have any questions.

Sincerely,



Walker & Armstrong, LLP
Phoenix, Arizona

Heber-Overgaard Unified School District

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

Audit purpose

To assess the District's efficiency and effectiveness in 4 operational areas—administration, plant operations and maintenance, food service, and transportation—and its compliance with certain State requirements.

Key findings

- District did not comply with important purchasing requirements, increasing its risk of unauthorized purchases and fraud.
- District did not ensure that all required personnel had fingerprint clearance cards and lacked a process to regularly confirm the validity of fingerprint clearance cards, increasing the risk to student safety.
- District did not safeguard and monitor the use of its fleet vehicles to prevent unauthorized use, theft, and damage.
- District assigned too much access to its accounting system and did not secure its information technology (IT) equipment, increasing its risk of errors, fraud, property damage, and data loss.

Key recommendations

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.
- Develop and implement a process to ensure that all required personnel have a valid fingerprint clearance card.
- 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.
- Limit employees' access to its accounting system to only those functions needed to perform their job duties and develop and implement written policies and procedures to limit and monitor physical access to its IT server room so that only appropriate personnel have access.

TABLE OF CONTENTS

District overview 1-2

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 3-6

Deficiency 1: District did not approve travel-related expenses in advance of travel

Deficiency 2: District failed to ensure all employees completed conflict-of-interest disclosure forms, limiting transparency and increasing the risk that District employees had not disclosed substantial interests that might influence or affect their official conduct

Deficiency 3: District did not ensure some employees had statutorily required fingerprint clearance cards and lacked a process to ensure fingerprint clearance cards were active

Deficiency 4: District did not secure personnel records, increasing its risk of unauthorized access to sensitive personnel information

Deficiency 5: District did not safeguard and monitor the appropriate use of some District property to prevent unauthorized use, theft, and damage

Recommendations

Finding 2: Districts excessive access to sensitive computerized data and other IT deficiencies increased the risk of unauthorized access to network and sensitive information, errors, fraud, and data loss 7-10

District has not complied with important IT security requirements and recommended practices

Deficiency 1: District’s passwords did not meet credible industry standards, putting District operations at risk

Deficiency 2: District assigned some users too much access to its accounting system, increasing its risk of errors and fraud

Deficiency 3: Terminated District employees had access to the District’s network, increasing the District’s risk of unauthorized access to sensitive information and data loss

Deficiency 4: District lacked a complete IT contingency plan, increasing the risk of data loss and disruptions to operations

Deficiency 5: District did not adequately secure its IT equipment, increasing its risk of property damage and data loss

District failed to develop and implement IT policies and procedures

Recommendations

TABLE OF CONTENTS

Summary of recommendations: W&A makes 20 recommendations to the District11-12


Appendix: Objectives, scope, and methodology a-1

District response

Table

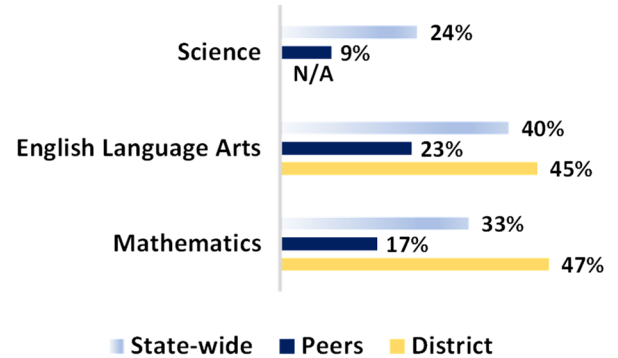
1 Criteria for selecting peer school districts for comparative purposes—Fiscal year 2022 a-2

Heber-Overgaard Unified School District—Performance Audit Fiscal Years 2022 and 2023 December 2023



Rural district in Navajo County
Grades: Kindergarten through 12th
FY 2022
Students attending: 461
Number of schools: 4
School letter grades¹: 2 Bs, 1 C

Students who passed State assessments²



¹ Source: Arizona State Board of Education 2021-2022. One District school did not receive a letter grade because it did not have a sufficient number of students.
² Source: *Arizona School District Spending Analysis—Fiscal year 2022*. Science data was not publicly available for the District due to Arizona Department of Education redaction requirements for student privacy.

FY 2022 total operational spending – \$5.7 million (\$12,339 per student)

Instructional – 62% (\$7,614 per student)

Noninstructional – 38% (\$4,725 per student)

Operational overview—FY 2022

	Measure	Heber-Overgaard USD	Peer average USD
<p>Administration—lower per student spending, but improvements needed</p> <p>The District spent less per student on administration than its peer districts averaged, primarily due to lower salary and benefit costs. However, the District allowed excessive access to its computerized and sensitive information and had other IT deficiencies, did not comply with certain purchasing and payroll requirements, and failed to safeguard District property. The District’s lack of controls and noncompliance with the USFR and State law resulted in unauthorized purchases and put other public monies and sensitive information at an increased risk of errors, fraud, unauthorized access, and data loss (see Findings 1 and 2, pages 3 through 10).</p>	Spending per student	\$1,684	\$2,050
<p>Plant operations—lower per square foot spending and no reported findings</p> <p>The District spent 28 percent less per square foot than its peer districts averaged, likely due to fewer personnel used to maintain their facilities. We did not report any findings in this area.</p>	Spending per square foot	\$4.94	\$6.34

<p>Food service—lower per meal spending and no reported findings</p> <p>The District spent less per meal on food service than its peer districts averaged. We did not report any findings in this area.</p>	<p>Spending per meal</p>	<p>\$4.01</p>	<p>\$4.33</p>
<p>Transportation—mixed spending and no reported findings</p> <p>The District had lower spending per mile and higher spending per rider on its transportation program than its peer districts averaged, indicating the District likely transported each of its riders more miles compared to its peers allowing the District to spread more costs over each mile. We did not report any findings in this area.</p>	<p>Spending per mile</p>	<p>\$1.93</p>	<p>\$3.10</p>
	<p>Spending per rider</p>	<p>\$2,199</p>	<p>\$2,035</p>

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

As part of our fiscal year 2022 review, we identified 5 primary deficiencies in the District's internal controls and failure to follow requirements set forth by the *Uniform System of Financial Records for Arizona School Districts* (USFR) and State law that resulted in unapproved purchases, potential undisclosed conflicts-of-interest, missing required personnel documentation, and inadequate safeguards for District property.³ See the details below.

Deficiency 1: District did not approve travel-related expenses in advance of travel

The USFR requires that districts prescribe procedures and amounts for reimbursing travel expenses and the District's policy required that any purchase, including for travel, must be approved prior to authorizing a purchase order. However, our review of 30 of 53 fiscal year 2022 travel expenditures found 3 payments that lacked documented approval prior to the travel. District officials could not provide an explanation for not following District policy for obtaining the required prior approval other than that the items identified had been overlooked. By not obtaining required approvals before travel purchases are made, the District increases the risk of unauthorized purchases or fraud.

Deficiency 2: District failed to ensure all employees completed conflict-of-interest disclosure forms, limiting transparency and increasing the risk that District employees had not disclosed substantial interests that might influence or affect their official conduct

State conflict-of-interest laws and District policy require public officers and employees to make known in official records and refrain from participating in any contract or matter for which the officer or employee has a substantial interest. State law and the USFR require districts to maintain a conflict-of-interest file for public inspection with information regarding governing board members' and employees' disclosed substantial interests. To meet USFR requirements, the District's conflict-of-interest policy

³ The Arizona Auditor General and the Arizona Department of Education developed the USFR pursuant to Arizona Revised Statutes (A.R.S.) §15-271. The USFR 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.

requires all board members to complete a conflict-of-interest disclosure form at the beginning of their term and annually thereafter. Similarly, the District requires employees to file a conflict-of-interest form within 5 days of commencing District employment and annually thereafter. The District’s annual employee training includes communicating conflict-of-interest laws and disclosure requirements. However, the District did not have a process in place to ensure that all board members and employees completed the form upon hire or annually, and therefore the District did not have completed conflict-of-interest disclosure forms for all employees. Our review of the District’s available conflict-of-interest disclosure forms for fiscal years 2022 and 2023 found that 78 and 69 employees, or approximately 51 and 45 percent of active District employees in each of these years, respectively, did not have a conflict-of-interest form on file, including the District’s superintendent and maintenance supervisor, both of whom are involved in authorizing and making District purchases.⁴

District officials responsible for maintaining conflict-of-interest disclosure forms indicated that it was difficult to track down certain individuals with inconsistent schedules, but otherwise could not explain the missing conflict-of-interest disclosure forms. However, the District had not implemented a process to monitor employees' and board members' compliance with its conflict-of-interest policy, which may have helped it to ensure employees and board members disclosed all required interests. By not ensuring employees complete conflict-of-interest disclosure forms upon hire or the beginning of their term and annually thereafter as required by District policy, the District cannot demonstrate that it is complying with State conflict-of-interest laws and increases the risk that District board members and employees had not disclosed substantial interest that might influence or affect their official conduct.

Deficiency 3: District did not ensure some employees had statutorily required fingerprint clearance cards and lacked a process to ensure fingerprint clearance cards were active

District policy requires all teachers and individuals that work in the classroom to have active fingerprint clearance cards.⁵ We reviewed personnel files for 33 of 183 fiscal year 2022 employees and identified 25 employees who, according to District policy, required an active fingerprint clearance card. However, our review found that the District lacked documentation to support that 2 of these employees had active fingerprint clearance cards, as required. Additionally, fingerprint clearance cards should be verified on the Department of Public Safety (DPS) website or by contacting DPS directly to ensure they are valid (see textbox). Regularly confirming the validity of fingerprint clearance cards is important because DPS

Fingerprint clearance card

A card issued by DPS after conducting a state and federal criminal background check to verify that prohibited criminal offenses such as sexual assault, child abuse or molestation, manslaughter, or kidnapping have not been committed. The card is valid for 6 years unless otherwise revoked. A copy of or the card itself is not evidence that a card is valid, so employers must regularly check the status of an individual’s card with DPS.

Source: Staff review of A.R.S. §§41-1758.02 and 41-1758.03 and the DPS website at <https://www.azdps.gov/services/public-services-portal/fingerprint-clearance-card>

⁴ All 5 Board members completed a conflict-of-interest disclosure form in each of these years.

⁵ Pursuant to A.R.S. §15-512(A), districts may require noncertified staff who are required or allowed to provide services directly to students without being supervised by a certified employee to obtain a fingerprint clearance card as a condition of employment.

may suspend/revoke the card if a cardholder is arrested/convicted of a precluding offense. However, the District lacked a process to regularly monitor and verify the validity of employees' fingerprint clearance cards.

The District could not explain why it did not have documentation to support that the 2 employees we identified had the required fingerprint clearance card. As described above, the District lacked important controls, such as a process to regularly monitor and verify employees' fingerprint clearance cards, which may have helped the District identify these deficiencies. By not ensuring employees required by District policy to have a fingerprint clearance card met that requirement and lacking a process to regularly monitor and verify the validity of employees' fingerprint clearance cards, the District increased risks to student safety because it cannot ensure that employees do not have criminal histories or offenses that would prohibit them from working with students.

Deficiency 4: District did not secure personnel records, increasing its risk of unauthorized access to sensitive personnel information

The USFR requires districts to maintain payroll records for all of its employees, and that these records be retained for the applicable period prescribed in accordance with the Arizona State Library and Archives' records retention schedules, which indicate that personnel records should be maintained for 5 years after an employee's termination. We reviewed bus driver credentials for all bus drivers employed by the District in fiscal years 2022 and 2023 and found that the District had not retained an employee file for 1 bus driver, as required. District officials stated that they were aware of the missing bus driver file prior to our review and indicated that when the employee resigned from the District to go work for another school district, a District employee had provided the entire original employee file to the individual upon termination. However, the District lacked important controls, such as a process to ensure the District secured employee files and limited access to only necessary personnel who were trained in confidentiality of sensitive employee information and file retention requirements, which may have prevented the District employee from improperly providing the bus driver's employee file to them upon their resignation. By not ensuring limited access to and retention of employee documentation, as required, the District increased the risk of noncompliance with USFR requirements and sensitive employee data being compromised.

Deficiency 5: District did not safeguard and monitor the appropriate use of some District property to prevent unauthorized use, theft, and damage

To safeguard district property from unauthorized use, theft, and damage, the USFR requires districts to implement physical security measures to restrict and monitor use of its property. Additionally, districts should restrict access to property to appropriate personnel. For vehicles, districts should implement and review detailed logs to track mileage to ensure the vehicles are used only for authorized district purposes. However, our review of District vehicles found that although the District's process required drivers to complete logs when they used District vehicles, the District could not provide usage logs to support that 11 of 20 vehicles were used appropriately and only for authorized District purposes. Due to a lack of documentation, we could not determine how much the District used these vehicles and for

what purpose. District officials reported that 2 of the vehicles were not actively used because they were assigned to specific employee positions that have remained unfilled; however, as previously discussed, the District lacked documentation necessary for us to determine the vehicles' usage. District officials further reported that some of the remaining fleet vehicles had been used to intermittently transport students in fiscal years 2022 and 2023 due to these vehicles not requiring driver certifications, and those drivers had not completed the logs, as required. However, the District lacked a process to monitor and review the logs to ensure District vehicles were used only for authorized purposes that may have helped it identify that drivers had not completed the logs and take action to ensure drivers tracked vehicle usage, as required. By not monitoring the use of its fleet vehicles, the District increased the risk of unauthorized use, theft, and damage of District property and cannot demonstrate that it used public resources only for authorized District purposes.

Recommendations

The District should:

1. 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.
2. 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.
3. 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.
4. 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.
 - b. Monitoring and regularly reviewing employees' fingerprint clearance cards to confirm their validity.
5. Secure and retain personnel files in accordance with applicable document retention schedules.
6. Develop and implement a process for appropriately providing personnel records to terminated employees and require training for responsible employees regarding the process.
7. 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.

District response: As outlined in its [response](#), the District agrees with the finding and recommendations and will implement the recommendations.

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

District has not complied with important IT security requirements and recommended practices

The USFR and credible industry standards, such as those developed by the National Institute of Standards and Technology (NIST), set forth important IT security practices that help districts safeguard sensitive information and prevent errors, fraud, and data loss. However, our review of the District's IT security practices identified several deficiencies, including noncompliance with USFR requirements and practices inconsistent with credible industry standards, that increased its risk for unauthorized access to sensitive information, errors, fraud, and data loss. See the details below.

Deficiency 1: District's passwords did not meet credible industry standards, putting District operations at risk

The USFR requires that districts implement strong passwords that align with credible industry standards. However, as of July 2023, some critical District systems' password requirements were not aligned with credible industry standards. As a result, the District increased the risk that unauthorized individuals could access sensitive District information and disrupt District operations.

Deficiency 2: District assigned some users too much access to its accounting system, increasing its risk of errors and fraud

The USFR requires districts to limit users' access to information and restrict access to only what is necessary for users to carry out their assigned duties. However, our July 2023 review of accounting system access levels for the 12 District employee accounts found that all 12 users had excessive access, allowing them to initiate and complete purchasing and/or payroll transactions without independent review. As a result, the District increased its risk for errors and fraud because these users could have completed payroll transactions or changes without a second employee to verify the payroll transactions or changes were accurate and appropriate. Additionally, the District granted administrator-level access to 5 users, including a business office employee, which gave the employees full access to view and edit all system information, further increasing the risk for errors and fraud. For example, users with administrator-level access have the ability to process false invoices; change employee payrates, including their own or add and pay nonexistent vendors without detection. In addition, the District

increased its risk of security breaches because hackers typically target administrator accounts for their greater access privileges, which could result in unauthorized access to and loss of sensitive data or disruption of some District operations. Although we did not identify any improper transactions due to these deficiencies within the accounting system, allowing such broad access increased the District's risk of errors and fraud. According to District officials, due to the District's limited staff, it was necessary for multiple people to have access to different modules in the accounting system. However, if adequate separation was not possible because of the District's limited staff, the District should have implemented additional management review procedures or other controls to compensate for allowing employees access to incompatible functions.

Deficiency 3: Terminated District employees had access to the District's network, increasing the District's risk of unauthorized access to sensitive information and data loss

The USFR requires that when user accounts are no longer needed, access to information systems be immediately disabled. However, our July 2023 review of the District's 120 active user accounts found that 10 network user accounts were active despite being associated with employees whose District employment had been terminated between 1 month and 4 years earlier. By allowing terminated employees access to its network, the District increased its risk of unauthorized access to its sensitive information and potential data loss. When we brought these accounts to the District's attention in July 2023, the District took no action. As of October 2023, the District had not assessed whether terminated employees accessed their accounts after they were no longer employed by the District.

Deficiency 4: District lacked a complete IT contingency plan, increasing the risk of data loss and disruptions to operations

As of July 2023, the District did not have a complete, up-to-date IT contingency plan. To help ensure continued operations and data recovery in the event of a system outage, the USFR requires and credible industry standards recommend that districts develop and implement an IT contingency plan. The plan should identify all critical systems, including the order in which they should be restored or criticality of the systems; clearly outline who is responsible for which activities during a system outage or attack; contain contingencies for continued business operations during a system outage; and contain detailed procedures for restoring critical systems and equipment. In addition to developing and implementing a comprehensive contingency plan, the District should test the plan at least annually to help ensure it is effective, which should include ensuring all employees understand their roles and responsibilities, identifying internal and external vulnerabilities, taking action to update equipment or remedy any issues identified, testing its ability to restore electronic data files for critical systems from backups, and documenting the results of the test. However, based on our July 2023 review, the District's plan did not contain some key components and the District did not regularly test its plan. Lacking a comprehensive and complete contingency plan exposes the District to an increased risk of being unable to continue operations and restore the District's systems in the event of a system outage.

Deficiency 5: District did not adequately secure its IT equipment, increasing its risk of property damage and data loss

The USFR requires that districts implement security-related controls over access to IT systems and data, including physical access. However, District officials could not provide information on who had access

to its computer servers and IT areas because there was no documentation for the number of keys that exist or who they were distributed to. Further, we observed the District's server room in July 2023 and identified water damage on the ceiling tiles of the server room. District IT staff indicated that the stained ceiling tiles were from previous leaks that had been repaired. However, maintenance personnel were unable to provide information on when the leaks occurred or evidence to support that a previous leak had been repaired. Allowing broad access to the server room and failing to properly protect computer equipment from hazards such as water damage increases the risk of interruptions to the District's network or operations, equipment loss, and possible loss of sensitive data.

District failed to develop and implement adequate IT policies and procedures

The District had not taken steps required by the USFR, such as developing policies and procedures, to ensure it complied with important IT security requirements. Although the District had some policies and procedures relating to IT, its policies and procedures were not adequate to prevent the deficiencies we identified. Additionally, according to District staff responsible for IT, the documented policies and procedures were not always consistent with the actual District operations in place and in some cases District staff were not aware of what the District's policy prescribed. For example, in response to our July 2023 review of password policies and requirements, District officials indicated they were not aware of what the District's password policy required and were not actively monitoring users' compliance with the District's policy.

Recommendations

The District should:

8. 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.
9. Develop and implement policies and procedures to review the District's password standards against industry password standards at least annually.
10. 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.
11. 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.
12. Immediately disable or remove all network accounts associated with terminated employees.
13. 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.

14. Establish written policies and procedures to ensure that terminated employees' network access is promptly removed.
15. 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.
16. Restrict physical access to its IT server room so that only appropriate personnel have access.
17. 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.
18. Conduct a physical inventory to determine and document the number of keys that exist and who has access to IT areas.
19. Perform regular inspections of IT areas for maintenance needs to protect property and data.
20. 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.

District response: As outlined in its [response](#), the District agrees with the finding and recommendations and will implement the recommendations.

SUMMARY OF RECOMMENDATIONS

Walker & Armstrong makes 20 recommendations to the District

The District should:

1. 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 (see Finding 1, pages 3 through 6, for more information).
2. 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 (see Finding 1, pages 3 through 6, for more information).
3. 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 (see Finding 1, pages 3 through 6, for more information).
4. 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.
 - b. Monitoring and regularly reviewing employees' fingerprint clearance cards to confirm their validity (see Finding 1, pages 3 through 6, for more information).
5. Secure and retain personnel files in accordance with applicable document retention schedules (see Finding 1, pages 3 through 6, for more information).
6. Develop and implement a process for appropriately providing personnel records to terminated employees and require training for responsible employees regarding the process (see Finding 1, pages 3 through 6, for more information).
7. 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 (see Finding 1, pages 3 through 6, for more information).
8. 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 (see Finding 2, pages 7 through 10, for more information).
9. Develop and implement policies and procedures to review the District's password standards against industry password standards at least annually (see Finding 2, pages 7 through 10, for more information).

10. 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 (see Finding 2, pages 7 through 10, for more information).
11. 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 (see Finding 2, pages 7 through 10, for more information).
12. Immediately disable or remove all network accounts associated with terminated employees (see Finding 2, pages 7 through 10, for more information).
13. 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 (see Finding 2, pages 7 through 10, for more information).
14. Establish written policies and procedures to ensure that terminated employees' network access is promptly removed (see Finding 2, pages 7 through 10, for more information).
15. 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 (see Finding 2, pages 7 through 10, for more information).
16. Restrict physical access to its IT server room so that only appropriate personnel have access (see Finding 2, pages 7 through 10, for more information).
17. 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 (see Finding 2, pages 7 through 10, for more information).
18. Conduct a physical inventory to determine and document the number of keys that exist and who has access to IT areas (see Finding 2, pages 7 through 10, for more information).
19. Perform regular inspections of IT areas for maintenance needs to protect property and data (see Finding 2, pages 7 through 10, for more information).
20. 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 (see Finding 2, pages 7 through 10, for more information).

Objectives, scope, and methodology

We have conducted a performance audit of Heber-Overgaard Unified School District on behalf of the Arizona Auditor General pursuant to A.R.S. §41-1279.03(A)(9). This audit focused on the District's efficiency and effectiveness primarily in fiscal year 2022, unless otherwise noted, in the 4 operational areas bulleted below because of their effect on instructional spending, as previously reported in the Arizona Auditor General's *Arizona School District Spending Analysis*. This audit was limited to reviewing instructional and noninstructional operational spending (see textbox). Instructional spending includes salaries and benefits for teachers, teachers' aides, and substitute teachers; instructional supplies and aids such as paper, pencils, textbooks, workbooks, and instructional software; instructional activities such as field trips, athletics, and co-curricular activities, such as choir or band; and tuition paid to out-of-State and private institutions. Noninstructional spending reviewed for this audit includes the following operational categories:

Operational spending

Operational spending includes costs incurred for the District's day-to-day operations. It excludes costs associated with acquiring capital assets (such as purchasing or leasing land, buildings, and equipment), interest, and programs such as adult education and community service that are outside the scope of preschool through grade 12 education.

- **Administration**—Salaries and benefits for superintendents, principals, business managers, and clerical and other staff who perform accounting, payroll, purchasing, warehousing, printing, human resource activities, and administrative technology services; and other spending related to these services and the governing board.
- **Plant operations and maintenance**—Salaries, benefits, and other spending related to equipment repair, building maintenance, custodial services, groundskeeping, and security; and spending for heating, cooling, lighting, and property insurance.
- **Food service**—Salaries, benefits, food supplies, and other spending related to preparing, transporting, and serving meals and snacks.
- **Transportation**—Salaries, benefits, and other spending related to maintaining school buses and transporting students to and from school and school activities.

Financial accounting data and internal controls—We evaluated the District's internal controls related to processing expenditures and scanned fiscal year 2022 payroll and accounts payable transactions in the District's detailed accounting data for proper account classification and reasonableness. Additionally, we reviewed detailed payroll and personnel records for 33 of 183 individuals who received payments through the District's payroll system in fiscal year 2022 and reviewed supporting documentation for 90 of 862 fiscal year 2022 accounts payable transactions. In addition, we reviewed fiscal year 2022 spending compared to the previous year and trends for the

different operational categories to assess reasonableness and identify significant changes in spending patterns. We also evaluated other internal controls that we considered significant to the audit objectives. This work included reviewing the District’s policies and procedures and, where applicable, testing compliance with these policies and procedures; reviewing controls over the District’s network and systems; and reviewing controls over reporting various information used for this audit. We reported our results on applicable internal control procedures in Findings 1 and 2 (see pages 3 through 10).

Peer groups—The Arizona Auditor General developed 3 types of peer groups for comparative purposes. To compare the District’s student achievement, the Arizona Auditor General developed a peer group using district type, location, and poverty rates because these factors are associated with student achievement. We used this peer group to compare the District’s fiscal year 2022 student passage rates on State assessments as reported by the ADE. We also reported the District’s fiscal year 2022 ADE-assigned school letter grade. To compare the District’s operational efficiency in administration, plant operations and maintenance and food service, the Arizona Auditor General developed a peer group using district size, type and location. To compare the District’s transportation efficiency, the Arizona Auditor General developed a peer group using a 5-year historical average of miles per rider and location. They used these factors because they are associated with districts’ cost measures in these areas.

Table 1

Criteria for selecting peer school districts for comparative purposes—Fiscal year 2022

Comparison areas	Factors	Group characteristics	Number of districts in peer group
Student achievement	Poverty rate District type Location	32% or higher but less than 35% Unified school districts Towns and rural areas	13
Administration, plant operations and maintenance, and food service	District size Location	200 to 499 students Towns and rural areas	15
Transportation	Miles per rider Location	511 to 720 miles per rider Towns and rural areas	17

Source: Staff review of the Arizona Auditor General’s district spending analysis—Fiscal year 2022.

Efficiency and effectiveness—In addition to the considerations previously discussed, we also considered other information that impacts spending and operational efficiency and effectiveness as described below:

- **Interviews**—We interviewed various District employees about their duties in the operational areas we reviewed. This included District and school administrators, department supervisors, and other support staff who were involved in activities we considered significant to the audit objectives.

- **Observations**—To further evaluate District operations, we observed various day-to-day activities in the operational areas we reviewed. This included facility tours, food services operations, and transportation services.
- **Report reviews**—We reviewed various summary reports of District-reported data including its Annual Financial Report, transportation safety reports provided by the Department of Public Safety, food-service-monitoring reports from ADE. We also reviewed District-provided accounting system and network user account reports and the fiscal year 2022 IT security awareness training roster.
- **Documentation reviews**—We reviewed various documentation provided by the District including: credit card and fuel card statements and supporting documentation for fiscal year 2022 purchases; cash receipts documentation and bank statements from July 2021 to June 2022, Governing Board meeting minutes; fiscal year 2022 employment contracts and payroll records; Board member and District employee conflict-of-interest disclosure forms for fiscal years 2022 and 2023; all available school bus driver files for fiscal years 2022 and 2023, 30 school bus preventative maintenance records, and pre- and post-trip bus inspection checklists for one week of each quarter for the District’s school buses for fiscal year 2022. We also reviewed Department of Public Safety school bus inspection reports for the school buses inspected in calendar years 2021 and 2022.
- **Analysis**—We reviewed and evaluated the District’s fiscal year 2022 spending on administration, plant operations and maintenance, food service, and transportation and compared it to peer districts. We also compared the District’s square footage per student, use of building space, and meals served per student to peer districts. Additionally, we reviewed the District’s food service program revenues and expenditures to evaluate the District’s ongoing ability to cover its food program costs and determine whether the District significantly subsidized its food service program with other District monies.

We selected our audit samples to provide sufficient evidence to support our findings, conclusions, and recommendations. Unless otherwise noted, the results of our testing using these samples were not intended to be projected to the entire population.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We express our appreciation to the District’s Board members, superintendent, and staff for their cooperation and assistance throughout the audit, as well as the Arizona Auditor General’s office for their support.

DISTRICT RESPONSE



Heber-Overgaard Schools

"Home of the Mustangs"

P.O. Box 547 Heber, Arizona 85928

Phone 928-535-4622 Fax 928-535-5146

www.heberovergaardschools.org

December 21, 2023

Walker & Armstrong LLP
1850 N. Central Ave., Ste 400
Phoenix, AZ 85004

To Whom It May Concern:

The Heber-Overgaard USD has received and reviewed the FY 20-21 / 21-22 / 22-23 Performance Audit Report. We would like to thank everyone on the audit team for their hard work and professionalism through this process.

After reviewing and discussing the audit findings and their recommendations we have addressed each area individually and have developed strategies and protocols moving forward. We believe these strategies will allow our district to enhance our performance and be more responsible as a school district that is entrusted to be fiscally responsible and to educate the wonderful students of our communities.

Please find attached the District's response to each finding and recommendation.

Respectfully,

Ron Tenney

Superintendent

Heber-Overgaard USD

Ph.: 928-535-4622

Email: ron.tenney@h-oschools.org

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

Recommendation 1: 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

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: We will review and update our procedures to be in compliance with USFR and District policy.

Recommendation 2: 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.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: For the audit years reviewed, we only gave forms to staff that attend orientation. FY23-24 we changed this procedure to include any employee that receives a paycheck. Policy for board member conflict of interest will be updated.

Recommendation 3: 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.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Recommendation 4: Develop and implement a process to ensure that all required personnel have a valid fingerprint clearance card, including:

Recommendation 4a: Maintaining documentation to support that all employees have fingerprint clearance cards if they are statutorily required to have one

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: District will use School ERP software to track all fingerprint clearance cards under the certification information. HR will review the list during Summer and Winter break to send out notifications to staff. HR will keep a list and verify all updated renewals as they come in. As well as identify those that have failed to renew.

Recommendation 4b: Monitoring and regularly reviewing employees' fingerprint clearance cards to confirm their validity

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Recommendation 5: Secure and retain personnel files in accordance with applicable document retention schedules.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Recommendation 6: Develop and implement a process for appropriately providing personnel records to terminated employees and require training for responsible employees regarding the process.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: Oversight on the transportation director part. Procedure put into place- Transportation director will make copies of the transportation file for staff that request it and keep the original copy for district records.

Recommendation 7: 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.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: For vehicles with a District Vehicle Authorization Form monthly logs will be turned into the transportation department. We have assigned an employee to physically verify mileage for all white fleet vehicles in the yard each day. This information is then verified and logged on a monthly spreadsheet maintained by the transportation director. Inventory for transportation supplies will be submitted yearly.

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

Recommendation 8: 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.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: ALL critical district password control systems have been aligned with credible industry standards. Two-factor authentication has been implemented since our audit.

Recommendation 9: Develop and implement policies and procedures to review the District's password standards against industry password standards at least annually.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: Each year during the Summer months administration along with IT will review the district password standards to verify conformance to the industry password standards. Any changes will be implemented before all staff returns for the following school year.

Recommendation 10: 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.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: We have cleaned up all the old staff accounts and are terminating access upon separation with the district. We have reviewed and adjusted all account access.

Recommendation 11: 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.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: We will review all accounts during the Summer break and Winter break to verify access and responsibilities. Any updates will be made and notifications emailed out before staff returns to work.

Recommendation 12: Immediately disable or remove all network accounts associated with terminated employees.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: Payroll will submit a ticket to IT with termination date. Checklists with all possible accounts will be reviewed before termination and IT will remove all access from any and all accounts within USFR guidelines.

Recommendation 13: 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.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: Any employee that has been terminated or resigned will have their account access removed immediately. The replacement or responsible employee will immediately be identified and all pertinent information will be transitioned. All transitioned accounts will be reviewed during Summer and Winter Break and removed.

Recommendation 14: Establish written policies and procedures to ensure that terminated employees' network access is promptly removed.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: Payroll will submit a ticket to IT with termination date. Checklists with all possible accounts will be reviewed before termination and IT will remove all access from any and all accounts within USFR guidelines.

Recommendation 15: 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.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: We will revamp our contingency plan within USFR guidelines. Training will be implemented for all new employees upon hire.

Recommendation 16: Restrict physical access to its IT server room so that only appropriate personnel have access.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: The IT server room will be re-keyed. A camera has been installed in the server room since our audit.

Recommendation 17: 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.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: We do have a physical tracking system, but failed to include the server rack keys. The key agreement has been updated to include all policies/procedures.

Recommendation 18: Conduct a physical inventory to determine and document the number of keys that exist and who has access to IT areas.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: An inventory has been done and all server rack keys have been identified and added to our key agreement.

Recommendation 19: Perform regular inspections of IT areas for maintenance needs to protect property and data.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: We will add an inspection of the server room and all network switch rooms to our Summer and Winter break duties and responsibilities list.

Recommendation 20: 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.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: Our IT Procedures will be revised and updated to comply with USFR guidelines.

