ARIZONA
AUDITOR GENERAL

LINDSEY A. PERRY
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

December 30, 2024

Members of the Arizona Legislature

The Honorable Katie Hobbs, Governor

Governing Board
Mammoth-San Manuel Unified School District

Ms. Julie Dale-Scott, Superintendent
Mammoth-San Manuel Unified School District

Transmitted herewith is a report of the Auditor General, *A Performance Audit of Mammoth-San Manuel 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 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 Dale-Scott 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

Mammoth-San Manuel Unified School District

District spent less than peer districts on administration, but lacked some required internal controls and did not comply with important IT security requirements, putting student safety, District property, and sensitive computerized data at risk

Performance Audit
A Report to the Arizona Legislature
December 2024
Report 24-213

Walker & Armstrong
CERTIFIED PUBLIC ACCOUNTANTS AND ADVISORS

Walker & Armstrong
CERTIFIED PUBLIC ACCOUNTANTS AND ADVISORS

December 19, 2024

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 Mammoth-San Manuel Unified School District for fiscal year 2023, conducted pursuant to Arizona Revised Statutes §41-1279.03.

As outlined in its response, the District agrees with all the findings and plans to implement or implement in a different manner 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

Walker & Armstrong, LLP
Phoenix, Arizona

Report Highlights

Walker & Armstrong
CERTIFIED PUBLIC ACCOUNTANTS AND ADVISORS

Mammoth-San Manuel Unified School District

District spent less than peer districts on administration, but lacked some required internal controls and did not comply with important IT security requirements, putting student safety, District property, 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 ensure that all required personnel had background checks and lacked a process to ensure personnel were trained on required employment documentation and retention requirements, increasing risks to student safety and noncompliance with federal law.
- District did not safeguard or monitor the use of its fleet vehicles to prevent unauthorized use, theft, and damage.
- District failed to limit access to its network and critical information systems and did not have a complete information technology (IT) contingency plan, increasing its risk of unauthorized access, errors, fraud, and data loss.

Key recommendations

The District should:

- Develop and implement policies and procedures for training employees on required hiring documentation and document retention timeframes to comply with federal law and the USFR.
- 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 user access to its network and critical information systems to only those functions needed to perform their job duties and develop and implement written policies and procedures to review system access and design an IT contingency plan to comply with USFR and credible industry standards.

See Performance Audit Report 24-213, December 2024, at www.azauditor.gov.

TABLE OF CONTENTS

Tables

Mammoth-San Manuel Unified School District—Performance Audit Fiscal Year 2023

December 2024

Rural district in Pinal County

Grades: Kindergarten through 12th

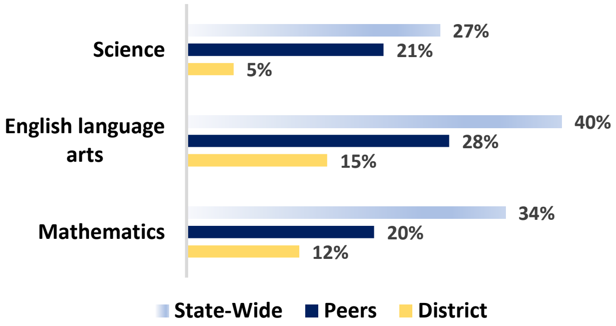
FY 2023

Students attending: 484

Number of schools: 3

School letter grades[1]: 2 Bs, 1 D

Students who passed State assessments[2]



[1] Source: Arizona State Board of Education 2022-2023.

[2] Source: *Arizona school district spending analysis—Fiscal year 2023.*

FY 2023 total operational spending – $6.7 million ($13,817 per student)

Instructional – 53% ($7,375 per student)	Noninstructional – 47% ($6,442 per student)

Operational overview—FY 2023	Measure	Mammoth-San Manuel USD	Peer average
Administration—lower per student spending and improvements needed The District spent less per student on administration than its peer districts averaged, primarily due to lower salaries and benefit costs. However, the District lacked important internal controls in some areas and did not comply with important IT standards, putting public monies and sensitive information at an increased risk of errors and fraud (see Findings 1 and 2, pages 3 through 9).	Spending per student	$1,670	$2,101
Plant operations—mixed spending and no reported findings The District's spending was similar to the average amount spent by its peer districts, with the District spending slightly less per square foot and more per student. We did not report any findings in this area.	Spending per square foot	$5.67	$6.65
	Spending per student	$2,179	$2,146

Operational overview—FY 2023	Measure	Mammoth-San Manuel USD	Peer average
Food service—mixed spending and no reported findings The District spent more per meal and less per student on food service than its peer districts averaged, likely due to fewer students participating in the District’s food service program. Per meal costs can be higher when participation is low because staffing and overhead costs still need to be covered. Lower participation can also affect the per student spending calculation since food service costs are calculated based on all students, not just those participating in the program. We did not report any findings in this area.	Spending per meal	$6.06	$5.34
	Spending per student	$590	$608
Transportation—mixed spending and improvements needed The District spent less per mile and more per rider on its transportation program than its peer districts averaged, primarily due to high salary and benefit costs, which accounted for $1,776 of the spending per rider. In addition, the District likely drove more miles transporting fewer students than its peer districts. Despite this increased spending on its transportation program, the District failed to maintain required transportation records for District vehicles (see Finding 1, pages 3 through 5).	Spending per mile	$3.82	$4.62
	Spending per rider	$2,732	$2,014

District lacked important internal controls in some areas, potentially increasing the risk to student safety and District property

As part of our review, we identified 2 deficiencies in the District's internal controls and failures to follow requirements set forth by the *Uniform System of Financial Records for Arizona School Districts* (USFR) and State and federal laws that resulted in missing required personnel documentation and the District's inability to demonstrate that it used fleet vehicles only for authorized purposes.[1] See the details below.

Deficiency 1: District lacked a process to ensure it retained required employment documentation for staff, resulting in missing evidence of required background checks for some District employees and potential noncompliance with federal law

State law requires all noncertified personnel, such as janitors, food service staff, and maintenance staff, to have a background check completed as a condition of District employment, but the District has not consistently complied with this requirement.[2] Background checks are important for ensuring that potential employees do not have criminal histories or offences that would prohibit them from working at the District. We reviewed personnel files for 30 of 154 employees who worked for the District in fiscal year 2023 and were required to have background checks as a condition of employment. Our review identified 2 employees for whom the District lacked documentation to support that it had completed required background checks.

The District could not explain why it did not have documentation supporting that it had conducted the required background checks for these 2 employees. The District uses a documentation checklist when onboarding new employees that outlines the documents that should be obtained for each new employee. However, for the 2 employees we identified, the District failed to follow its process to ensure it collected all required documentation before they began working at the District. By failing to follow its process to ensure that all documentation is completed before the individuals began employment, the District potentially increased the risk to student safety.

Similarly, federal law requires every employer who hires an individual to obtain a Form I-9, *Employment Eligibility Verification*, and requires that employers retain the form for 3 years after the date

[1] The Arizona Auditor General and the Arizona Department of Education (ADE) 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.

[2] A.R.S. §15-512.

of hire or 1 year after the date employment is terminated, whichever is later.[3] Additionally, the USFR requires districts to maintain employee payroll records for 5 years after an employee's termination. Our review of 30 of 154 employees who worked at the District in fiscal year 2023 found 5 instances in which the District did not have documentation to support that a Form I-9 was completed to verify the employee's eligibility to work in the United States.

District officials stated they were unaware of the requirement to complete an eligibility verification for 3 students it hired for the District's Community Schools program. Additionally, although the I-9 form is included on the District's documentation checklist, District officials could not explain why the other 2 employee files did not contain the required documentation. Based on our review, the District lacked a process for ensuring that District personnel were trained in hiring and file retention requirements, which may have helped to ensure that staff obtained and/or retained required employment documentation. By not ensuring employee documentation was completed and retained as required, the District increased the risk of hiring personnel not authorized to work in the United States and noncompliance with federal law and USFR requirements.

Deficiency 2: District did not safeguard or monitor the appropriate use of District property to prevent unauthorized use, theft, and damage

To safeguard school 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, but the District has not done so.

Our review of District fleet 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 for any of its fleet vehicles in response to our requests. Due to a lack of documentation, we could not determine how much the District used these vehicles and whether the vehicles were used only for authorized District purposes. In addition to not enforcing the requirement for staff to complete the fleet vehicle usage logs, the District also lacked a process to monitor and review the usage logs to ensure District vehicles were used only for authorized purposes. Such a process may have made the District aware that drivers had not completed the logs and enabled it to 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. Review personnel files for employees who are required to have background checks to ensure that all required checks have been completed and documented.

2. Follow its process to complete an onboarding checklist for all newly hired employees.

[3] Title 8, CFR §274a.2.

3. Develop and implement policies and procedures for training employees on required hiring documentation and document-retention time frames to comply with federal law and the USFR.

4. Retain documentation in personnel files in accordance with applicable document-retention schedules.

5. Develop and implement policies and procedures for monitoring and reviewing usage logs for all District vehicles that includes ensuring vehicles are used only for an authorized purpose.

District response: As outlined in its response, the District agrees with the finding and recommendations and will implement the recommendations.

FINDING 2

District's excessive access to its sensitive computerized data and other IT deficiencies increased the risk of unauthorized access to its network and sensitive information, errors, fraud, and data loss

District has not complied with important IT security requirements and credible industry standards

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, data loss, errors, and fraud. See the details below.

Deficiency 1: District did not regularly review and limit user access to its network and critical systems, increasing its risk of unauthorized access to sensitive information, data loss, errors, and fraud

The USFR requires that districts limit users' access to information and restrict the types of access to only what is necessary for users to carry out their assigned duties. The USFR further requires that when user accounts are no longer needed, such as when an employee terminates from district employment, access to information systems should be immediately disabled. Although credible industry standards recommend districts develop policies and procedures to regularly review and limit user access, the District has not done so.

Our July 2024 review of accounts on the District's network, student information system (SIS), and accounting information system (AIS) found the District did not regularly review and limit users' access to only what they need to perform job duties (see Table 1, page 7). Specifically:

- **District did not limit the number of SIS users with administrator-level access**—Our review of 7 of 30 users of the student information system found 1 user's access was more than necessary to perform their job duties. Specifically, an outside consultant had administrator-level access to the SIS, which gave them access to sensitive student information and the ability to make changes to the system, including changing user access levels. According to District officials, the outside consultant could complete their job duties with view-only access. We informed the District of the issue in July 2024, and this account has since been updated to view-only access.

- **District did not ensure AIS users had only access necessary to perform their job duties**—Our review of 5 of 20 users of the AIS found that 4 users had access that was more than what was necessary to perform their job duties. Specifically, we found that 3 AIS users had the ability to view and modify employee information and pay rates, including their own, as well as initiate and complete payroll and purchasing transactions without another employee reviewing and approving the transactions. In addition, we found that another user, a business office employee, was granted full access to the District's accounting system. This level of access gave the employee the ability to process false invoices; change employee pay rates, including their own; or add and pay nonexistent vendors or employees without detection.

  District officials reported that, prior to our review, it was not aware that any users had excessive access to the AIS. The District also indicated that, due to limited staffing, 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 staffing limitations, the District should have implemented additional management review procedures or other compensating controls, such as a process for a supervisor to regularly review system logs, balancing reports, and other relevant indicators, consistent with USFR requirements.

- **District did not promptly remove accounts that were no longer needed**—Our review of 8 of 153 users of the District's network found 2 user accounts that appear to have been associated with vendors that no longer needed access to the network because they no longer provided services to the District. The District could not provide information about when the accounts should have been disabled, but our review found 1 of the accounts was last accessed approximately 3 years ago and the other more than 9 years ago.

Although we did not identify any improper transactions due to these deficiencies, system access beyond what is needed for an employee's job duties and failure to remove access when it is no longer needed increases the risk of errors and fraud.

Table 1: District's management of user access controls

Requirement	Network	Student Information System	Accounting Information System	Summary
Limit the number of users with administrator-level access	✓	X	✓	We found that 1 SIS user account associated with a District consultant had administrator-level access, but this level of access was not needed to perform their job duties.
Restrict user access to what is necessary to perform job duties	✓	X	X	We found that 4 of 5 AIS users we reviewed and 1 of 7 SIS users we reviewed had more system access than necessary to perform their job duties.
Remove account access once access is no longer necessary	X	✓	✓	We found that at least 2 network user accounts were associated with discontinued vendor accounts but had not been disabled.

Source: Walker & Armstrong staff analysis of District information systems.

Deficiency 2: District's authentication controls did not align with credible industry standards, increasing the risk of unauthorized access to sensitive information and disruptions to operations

The USFR requires that districts implement strong passwords that align with credible industry standards. However, as of July 2024, 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.

After bringing these issues to the District's attention during the audit, District staff immediately updated system policies to align with credit industry standards, which we confirmed during our review. Additionally, the District reported that it is in the process of working to implement multifactor authentication for its systems.

Deficiency 3: District lacked a complete IT contingency plan, increasing the risk of data loss and disruptions to operations

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 test results.

Based on our July 2024 review, the District's IT contingency plan lacked some key components. Specifically, the District's IT contingency plan had incomplete, missing, or outdated information for several critical components, including:

- An impact analysis to assess the likelihood of potential disasters, including possible consequences, and the necessary remedial actions.
- An inventory of equipment, software, vital records and supplies required to resume operations.
- A crisis-management plan outlining the District's response strategy.
- Escalation procedures detailing how to identify and respond to emergencies effectively.

Additionally, the District did not test its plan at least annually to help ensure it was effective and that each staff member knew their responsibilities in the event of an emergency that affected the District's IT systems. The District reported that it did not have a complete and up-to-date IT contingency plan because it prioritized other items over these tasks. However, the lack of such a plan increases the risk that the District will be unable to continue operations and restore its systems in the event of a system outage.

Recommendations

The District should:

6. Protect its sensitive computerized data by limiting users' access to its accounting system and student information system to only those functions needed to perform their job duties, including removing the outside consultant's administrator-level access and business office employees' full access.
7. 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.
8. Immediately disable or remove all unnecessary user accounts in its network and implement a review process to ensure network access is removed immediately when an employee or vendor relationship is terminated.
9. Develop and implement an IT contingency plan that meets USFR requirements and credible industry standards, test the plan at least annually to identify and remedy deficiencies, and document the test results.

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 9 recommendations to the District

The District should:

1. Review personnel files for employees who are required to have background checks to ensure that all required checks have been completed and documented (see Finding 1, pages 3 through 5, for more information).
2. Follow its process to complete an onboarding checklist for all newly hired employees (see Finding 1, pages 3 through 5, for more information).
3. Develop and implement policies and procedures for training employees on required hiring documentation and document-retention time frames to comply with federal law and the USFR (see Finding 1, pages 3 through 5, for more information).
4. Retain documentation in personnel files in accordance with applicable document-retention schedules (see Finding 1, pages 3 through 5, for more information).
5. 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 5, for more information).
6. Protect its sensitive computerized data by limiting users' access to its accounting system and student information system to only those functions needed to perform their job duties, including removing the outside consultant's administrator-level access and business office employees' full access (see Finding 2, pages 6 through 9, for more information).
7. 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 6 through 9, for more information).
8. Immediately disable or remove all unnecessary user accounts in its network and implement a review process to ensure network access is removed immediately when an employee or vendor relationship is terminated (see Finding 2, pages 6 through 9, for more information).
9. Develop and implement an IT contingency plan that meets USFR requirements and credible industry standards, test the plan at least annually to identify and remedy deficiencies, and document the test results (see Finding 2, pages 6 through 9, for more information).

APPENDIX

Objectives, scope, and methodology

We have conducted a performance audit of Mammoth-San Manuel 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 2023, 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 annual *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.

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.

Noninstructional spending reviewed for this audit includes the following operational categories:

- **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, 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 2023 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 30 of 154 individuals who received payments through the District's payroll system in fiscal year 2023 and reviewed supporting documentation for 70 of 3,983 fiscal year 2023 accounts payable transactions. In addition, we reviewed fiscal year 2023 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 Finding 1 (see pages 3 through 5).

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 2023 student passage rates on State assessments as reported by ADE. We also reported the District's fiscal year 2023 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 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 2: Criteria for selecting peer school districts for comparative purposes—Fiscal year 2023

Comparison areas	Factors	Group characteristics	Number of districts in peer group
Student achievement	Poverty rate District type Location	16% or higher but less than 23% Unified school districts Towns and rural areas	14
Administration, plant operations and maintenance, and food service	District size District type Location	200 to 499 students Unified school districts Towns and rural areas	16
Transportation	Miles per rider Location	341 to 515 miles per rider Towns and rural areas	18

Source: Walker & Armstrong staff review of the Arizona Auditor General's *Arizona School District Spending Analysis–Fiscal year 2023*.

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*, Single Audit reports, and compliance questionnaire results that its external financial audit firm completed. We also reviewed District-provided accounting system and network user account reports and documentation related to the District's fiscal year 2023 IT security-awareness training.
- **Documentation reviews—**We reviewed District-provided documentation, including credit card statements and supporting documentation for fiscal year 2023 purchases; cash receipts documentation and bank statements from July 2022 to June 2023; Governing Board meeting minutes; fiscal year 2023 employment contracts and payroll records; Governing Board member and District employee conflict-of-interest disclosure forms for fiscal year 2025; and all school bus driver files for fiscal year 2023. We also reviewed Department of Public Safety school bus inspection reports for the school buses inspected in calendar years 2022 and 2023.
- **Analysis—**We reviewed and evaluated the District's fiscal year 2023 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.

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 Governing 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

MAMMOTH-SAN MANUEL UNIFIED SCHOOL DISTRICT
POST OFFICE BOX 406
SAN MANUEL, ARIZONA 85631
(520) 385-2336
FAX (520) 385-2621

SUPERINTENDENT
Julie Dale-Scott

December 19, 2024

Lisa S. Parke, CPA
Audit & Assurance Partner
Walker & Armstrong
1850 N. Central Avenue, Suite 400
Phoenix, AZ 85004

Dear Ms. Parke:

Please accept Mammoth-San Manuel Unified School District's response to the performance audit that has recently been completed. The administration and governing board accept the findings, have already implemented some recommendations and will continue to diligently work to implement the remaining recommendations.

The District would like to share our appreciation to the audit team for their professionalism and patience while conducting the audit. Thank you for working with us in such a positive way that helped us grow through this process.

Sincerely,

Julie A Dale Scott

Julie Dale-Scott
Superintendent

Finding 1: District lacked important internal controls in some areas, potentially increasing the risk to student safety and District property.

District Response: The finding is agreed to.

Recommendation 1: Review personnel files for employees who are required to have background checks to ensure that all required checks have been completed and documented.

District Response: The audit recommendation will be implemented.

Recommendation 2: Follow its process to complete an onboarding checklist for all newly hired employees.

District Response: The audit recommendation will be implemented.

Recommendation 3: Develop and implement policies and procedures for training employees on required hiring documentation and document-retention time frames to comply with federal law and the USFR.

District Response: The audit recommendation will be implemented.

Recommendation 4: Retain documentation in personnel files in accordance with applicable document-retention schedules.

District Response: The audit recommendation will be implemented.

Recommendation 5: 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 audit recommendation will be implemented.

Finding 2: District's excessive access to its sensitive computerized data and other IT deficiencies increased the risk of unauthorized access to its network and sensitive information, errors, fraud, and data loss.

District Response: The finding is agreed to.

Recommendation 6: Protect its sensitive computerized data by limiting users' access to its accounting system and student information system to only those functions needed to perform their job duties, including removing the outside consultant's administrator-level access and business office employees' full access.

District Response: The audit recommendation will be implemented.

Response explanation: The District is working on implementing this recommendation and have removed access for the consultant whose account was identified in the audit.

Recommendation 7: 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 audit recommendation will be implemented.

Recommendation 8: Immediately disable or remove all unnecessary user accounts in its network and implement a review process to ensure network access is removed immediately when an employee or vendor relationship is terminated.

District Response: The audit recommendation will be implemented.

Recommendation 9: Develop and implement an IT contingency plan that meets USFR requirements and credible industry standards, test the plan at least annually to identify and remedy deficiencies, and document the test results.

District Response: The audit recommendation will be implemented.

Response explanation: The district added a two-factor authentication (2FA) service that adds an extra layer of security in September 2024.

Walker & Armstrong

CERTIFIED PUBLIC ACCOUNTANTS AND ADVISORS