Mohave Valley Elementary School District

> **District subsidized its food service program with over $167,000 that it could have spent on instruction, overpaid some employees, did not ensure all cash collected was deposited, and did not adequately protect its computerized data**

Audit purpose

To assess the District's spending on administration, plant operations and maintenance, food service, and transportation and its compliance with certain State requirements.

Key findings

- District subsidized its food service program in fiscal years 2017 through 2019 with over $167,000 that it could have spent on instruction.

- District's decision to participate in the federal Community Eligibility Program (CEP) that provides free meals to all students caused food service program financial loss.

- District likely could have increased its revenues $110,000 per year by participating in the standard National School Lunch Program (NSLP) instead of the CEP.

- District overpaid 4 employees a total of almost $5,700 because its payroll process did not have a comprehensive secondary review.

- District did not ensure all cash collected was deposited and in a timely manner, leading to an increased risk of errors and fraud.

- District did not adequately protect its computerized data, which increased risk of unauthorized access to sensitive information, errors, fraud, and data loss.

Key recommendations

The District should:

- Analyze whether participation in the NSLP rather than the CEP would be financially beneficial, and take action to ensure its food service program revenues cover program costs.

- Strengthen its payroll process by having a second person review payroll information to ensure employees are paid accurately.

- Provide training on cash-handling requirements to employees, have an employee review supporting documentation for all cash collected, and deposit all cash at least weekly.

- Better protect its sensitive computerized data from unauthorized access, errors, fraud, and data loss by implementing and enforcing strong password requirements, reducing the number of users with administrator-level access, limiting users' access in its accounting system, removing all unnecessary network user accounts, and reviewing and testing its IT contingency plan.