

Nogales Unified School District No. 1



November 3, 2016

State of Arizona
Office of Auditor General
2910 N. 44th Street, Suite 410
Phoenix, AZ 85018

Re: Preliminary Draft Performance Audit FY2014

Dear Ms. Orrico,

The Nogales Unified School District has received and reviewed the Preliminary Draft Performance Audit conducted for the fiscal year 2014. NUSD would like to express sincere appreciation for the professionalism shown by the Auditor General's staff throughout the audit process as well as during follow-up discussions in which staff provided clarification regarding the audit findings.

The information shared with the District during the exit interview and in subsequent dialogues have provided the district with the opportunity to reflect upon practices and procedures which are in place pertaining to systems security and operations, transportation, and building access. The recommendations provided in the Performance Audit were welcomed and will be utilized to address deficiencies and improve operations. It is the intent of the District to use the recommendations provided in the Auditor General's report to address all findings and move quickly into compliance.

Sincerely,

Fernando Parra
Superintendent

Finding 1: District lacked adequate controls to protect it from errors, fraud, and unauthorized access to sensitive information

District Response: Although no errors, fraud or unauthorized access to sensitive information was detected or found to have occurred, the District agrees with the finding and recommendations, recognizing that there were some areas in which adequate controls were lacking. However, the District took immediate action to remediate each of the deficiencies identified to protect the District integrity.

Recommendation 1: The District should implement and enforce stronger password requirements for its student information system related to password length, complexity, and expiration, and only the user should know his/her password.

District Response: The District has already taken steps to be in compliance with the requirement to implement and enforce stronger passwords for the student information system by utilizing best practices for creating strong passwords as described in the recommendation and by ensuring that passwords are required to be regularly reset at appropriate time intervals as well as after initial creation for staff by administrative users.

Recommendation 2: The District should limit employees' access to its accounting system to only those accounting system functions needed to perform their work. Further, the District should ensure that employees with access to the accounting system each have only one user account.

District Response: The District recognizes that employee access to the accounting system should be restricted to those functions necessary to complete their job responsibilities and to avoid access to all three system modules (purchasing/payables, human resources, and payroll). The access level of the twelve employees referenced has been reviewed and action has been taken to limit access and user roles for all twelve employees to only those which are needed to complete job duties and to avoid "full access" to the accounting system by any one employee. Additionally, the District has begun to regularly review employee access to the accounting system to ensure user access is appropriate for current job duties.

Recommendation 3: The District should review and consider reducing the number of users with administrator-level access to its network and systems.

District Response: The District has reviewed administrator-level access to both the network and student information systems. With regards to the sixteen network users which had administrator-level access, all of the user accounts cited have been reviewed. Three were identified as district technology department employees with domain-level administrative access that was deemed as necessary to perform job duties. Seven accounts were identified as vendor network support accounts that are not typically needed and have been disabled. The remaining six network users were identified as site-level computer staff accounts whose access could be more restricted. The District is in the process of decreasing user rights for these accounts by assigning more restricted access. With regards to the student information system accounts whose access level was in question, the two administrator-level accounts were re-examined and have been removed as recommended.

Recommendation 4: The District should develop and implement a formal process to ensure that terminated employees have their computer network and systems access promptly removed.

District Response: Auditors identified both network and student information system accounts linked to former employees which had not been disabled or deleted upon termination of employment. Action was immediately taken on the twenty-two network user accounts and all of the accounts were deleted with verification of the action provided to auditors. Similarly, for the twenty-three student information system accounts, all identified user accounts have been disabled. Furthermore, standard operating procedures to maintain control and handling of user accounts for terminated employees has been revised and implemented to ensure prompt removal of access when a user is no longer employed with the District. This revised procedure will be added to the IT Internal Control Policy Manual.

Recommendation 5: The District should eliminate unnecessary shared user accounts in its network and systems and properly control any remaining shared accounts, such as disabling them when not being used.

District Response: Auditors identified three network and three student information system accounts which were not assigned to particular individuals and may have been utilized as shared accounts. With regards to the three network accounts, the District has removed all three network accounts identified as potentially unnecessary. One account was created at employees' request which did allow shared access; however, this account was deleted to be in compliance with the recommendation. The two remaining network accounts were system accounts for application background services that are no longer needed.

In response to the three student information system accounts, two of the accounts identified are not in use and cannot be deleted from the system. One is a default user group created by the vendor and the second was created for monitoring by a previous administrator. However, both of the unassigned accounts have been disabled and/or severely restricted to prevent user access. The third account is a domain-level user account which was created by the vendor and cannot be deleted. However, this account has been deemed as necessary to recover system access by essential domain-level users.

Recommendation 6: The District should establish and implement policies and procedures for logging and monitoring users' activities on its network and critical systems.

District Response: To implement this recommendation, the District will enable the logging functions within the network's active directory to allow monitoring of user activity. The audit logs produced will be analyzed on a regular basis to ensure recommendation compliance. Additionally, the District is currently drafting procedures for logging and monitoring network activity which will be included in the IT Internal Control Policy Manual.

Recommendation 7: The District should implement controls to limit employees' ability to install unauthorized software on district computers or develop a process to monitor computers for installation of unauthorized software.

District Response: The District has implemented the use of an existing group policy that currently restricts certain peer-to-peer applications from running and will add restrictions that will control the installation of unauthorized applications. Additionally, the District will use Antivirus Suite functionality that detects and reports potentially unwanted applications from being installed and run. The District will review these reports on a continuous basis to better control applications being installed or attempted to be installed. The District will also work on developing procedures for logging and monitoring users' activities on the network.

Recommendation 8: The District should review its formal contingency plan to ensure it is complete and test it periodically to identify and remedy deficiencies.

District Response: The District has begun to revise the current contingency plan to include key components (e.g. system recovery, plan testing, and contact information) delineated in the findings. The plan is being updated to provide necessary contact information for staff assigned by role/function with specific responsibilities during an equipment or system failure/interruption. A recovery plan for critical systems is being developed to prevent disruptions of system operations. Once the recovery plan has been completed, a testing plan will also be articulated and implemented.

Recommendation 9: The District should implement controls over its process for distributing and tracking building keys, including maintaining a complete and up-to-date distribution log, establishing a process for determining the access level given to employees, and implementing a user agreement outlining the rules and policies an employee must follow regarding the use of district keys.

District Response: To address this recommendation, the District immediately took action following the preliminary audit exit report to ensure the District maintains control over building access. The District has developed a manual that very clearly defines how keys will be made, issued and tracked at all campuses and district offices. Support Services will maintain a master control log of all keys that have been issued to each school and department. Additionally, Support Services is responsible for monitoring who should have keys and site administrators must justify, through a written key request, for whom they are requesting keys to be made. A key user agreement has been developed for all key holders that clarifies the terms and conditions for key usage. Support Services will annually collect and compare site key logs with the master key log to ensure any changes have been updated on both logs.

Finding 2: District needs to improve transportation program oversight and may be able to reduce costs

District Response: The District agrees with the finding and recommendations, recognizing that the ability to conduct a more detailed analysis of all transportation costs would provide an opportunity for the identification of areas for possible cost savings.

Recommendation 1: The District should work with its transportation vendor to determine whether the vendor's billings could be modified to provide more detail by breaking out daily rates and additional trip costs by cost categories, including salaries and benefits, maintenance and repairs,

bus rental costs, and supplies, and have the vendor modify the billings accordingly. Additionally, the District should use this information to determine areas where cost savings can be achieved.

District Response: The District has already contacted the transportation vendor to discuss obtaining more detailed billing information that had not been clearly defined on the bid. However, the District is confident that the invoices from the vendor can be modified to provide more detail and enable the District to become in compliance with the recommendation. The District will request that the transportation invoices include the following: trip costs, salaries/benefits, bus rental costs, and maintenance/repairs. The District will also request that the vendor provides monthly student counts for each bus route.

Additionally, the District has already taken other steps to minimize transportation costs by utilizing in-house drivers and small district vehicles to provide transportation, when it is required, to special education students that must be transported to educational facilities in Tucson for services.

By holding the vendor accountable for submitting detailed invoices and data, as well as re-evaluating and/or renegotiating the rates outlined in the vendor contract and utilizing district drivers/vehicles whenever feasible, the District may be able to achieve cost savings

Recommendation 2: The District should review its bus routes to determine if it can improve route efficiency and adjust its bus routes accordingly.

District Response: The District agrees that an ongoing review of routes can improve efficiency and may provide costs savings. During FY15, the District performed an internal audit for the contracted buses and associated routes. Support Services employees did a “ride along”, boarding different buses at the start of the school day and at the end of the school day for a week during August of 2014. The District monitored all bus routes and during this study it was discovered that one of the Special Education routes could be eliminated and student transportation would be just as efficient. However, the FY15 internal audit revealed that none of the buses for regular routes could be eliminated; it was determined that it would not be cost effective to eliminate a regular bus as the pick-up and drop-off times for students would be negatively impacted. However, in FY17 continued monitoring of bus routes and the number of students actually transported revealed that a regular bus could now be eliminated to produce cost savings. The District has been proactive in trying to identify if routes are efficient and if any changes need to be made to provide cost savings to the District.

Recommendation 3: The District should develop and monitor performance measures such as cost per mile, cost per rider, and bus capacity usage to better evaluate and improve the efficiency of its transportation program.

District Response: The District has been working diligently during negotiations of our transportation contract to ensure the efficiency of the program. The District is cognizant that transportation costs did increase during FY14 as corrective actions were taken with regards to the coding of transportation expenditures. It is recognized that the cost per mile

and cost per student is higher than peer districts and that implementing performance measures as recommended would be beneficial. The District is closely monitoring and analyzing student transportation data through internal audits to identify areas in which the cost of operations can be reduced. The District will continue to explore and implement strategies, such as more detailed monthly invoicing and internal audits, to detect areas for possible adjustments to decrease costs and improve the efficiency of student transportation. As previously mentioned, the District is also re-evaluating the terms and conditions outlined in the vendor contract to obtain transportation savings.

Recommendation 4: The District should develop a formal preventative maintenance policy that meets the State's *Minimum Standards* and includes the maximum number of miles and the maximum amount of time a bus can travel before it receives preventative maintenance services. Additionally, the District should ensure that it conducts bus preventative maintenance in a systematic and timely manner and documents it in accordance with its formal policy.

District Response: The District has already begun to implement preventative maintenance policies for buses identified in the recommendations to meet State's Minimum Standards. The District will ensure that Support Services maintains and follows the maintenance guidelines as clearly defined in the owner's manual for the maintenance of buses. Each district-owned bus will be serviced every 3000 miles or 500 hours of operation, whichever comes first. The District will also ensure that a log book is maintained as per the State Minimum Standards for all District-owned buses to document that Support Services has maintained and serviced all buses as required. The District will continue to implement necessary changes to comply with the State Minimum Standards and demonstrate compliance with the recommendation.