Mohave County Community College District

Single Audit Report

Year Ended June 30, 2016

A Report to the Arizona Legislature

Debra K. Davenport
Auditor General

ARIZONA
AuditorGeneral
Making a Positive Difference

The Auditor General is appointed by the Joint Legislative Audit Committee, a bipartisan committee composed of five senators and five representatives. Her mission is to provide independent and impartial information and specific recommendations to improve the operations of state and local government entities. To this end, she provides financial audits and accounting services to the State and political subdivisions, investigates possible misuse of public monies, and conducts performance audits and special reviews of school districts, state agencies, and the programs they administer.

The Joint Legislative Audit Committee

Senator **Bob Worsley**, Chair
Senator **Judy Burges**
Senator **John Kavanagh**
Senator **Sean Bowie**
Senator **Lupe Contreras**
Senator **Steve Yarbrough** (ex officio)

Representative **Anthony Kern**, Vice Chair
Representative **John Allen**
Representative **Rusty Bowers**
Representative **Rebecca Rios**
Representative **Athena Salman**
Representative **J.D. Mesnard** (ex officio)

Contact Information

Arizona Office of the Auditor General
2910 N. 44th St.
Ste. 410
Phoenix, AZ 85018

(602) 553-0333

www.azauditor.gov

TABLE OF CONTENTS

Auditors Section

Report Issued Separately

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

Independent auditors' report on internal control over financial reporting and on compliance and other matters based on an audit of basic financial statements performed in accordance with *Government Auditing Standards*

Members of the Arizona State Legislature

The Governing Board of
Mohave County Community College District

We have audited the financial statements of the business-type activities and discretely presented component unit of Mohave County Community College District as of and for the year ended June 30, 2016, and the related notes to the financial statements, which collectively comprise the District's basic financial statements, and have issued our report thereon dated January 19, 2017. Our report includes a reference to other auditors who audited the financial statements of the Mohave Community College Foundation, the discretely presented component unit, as described in our report on the District's financial statements. We conducted our audit in accordance with U.S. generally accepted auditing standards and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. However, the financial statements of the Mohave Community College Foundation were not audited in accordance with *Government Auditing Standards*, and accordingly, this report does not include reporting on internal control over financial reporting or instances of reportable noncompliance associated with the Mohave Community College Foundation.

Internal control over financial reporting

In planning and performing our audit of the financial statements, we considered the District's internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the basic financial statements, but not for the purpose of expressing an opinion on the effectiveness of the District's internal control. Accordingly, we do not express an opinion on the effectiveness of the District's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies, and therefore, material weaknesses or significant deficiencies may exist that were not identified. However, as described in the accompanying schedule of findings and questioned costs, we identified certain deficiencies in internal control that we consider to be material weaknesses and significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the District's basic financial statements will not be prevented, or detected and corrected, on a timely basis. We consider the deficiency described in the accompanying schedule of findings and questioned costs as item 2016-01 to be a material weakness.

A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider the deficiencies described in the accompanying schedule of findings and questioned costs as items 2016-02, 2016-03, 2016-04, 2016-05, 2016-06, and 2016-07 to be significant deficiencies.

Compliance and other matters

As part of obtaining reasonable assurance about whether the District's basic financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

Mohave County Community College District's response to findings

Mohave County Community College District's responses to the findings identified in our audit are presented in its corrective action plan at the end of the report. The District's responses were not subjected to the auditing procedures applied in the audit of the basic financial statements, and accordingly, we express no opinion on them.

Purpose of this report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the District's internal control or on compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the District's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Jay Zsorey, CPA
Financial Audit Director

January 19, 2017

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

Independent auditors' report on compliance for each major federal program; report on internal control over compliance; and report on schedule of expenditures of federal awards required by the Uniform Guidance

Members of the Arizona State Legislature

The Governing Board of
Mohave County Community College District

Report on compliance for each major federal program

We have audited Mohave County Community College District's compliance with the types of compliance requirements described in the *U.S. Office of Management and Budget (OMB) Compliance Supplement* that could have a direct and material effect on each of its major federal programs for the year ended June 30, 2016. The District's major federal programs are identified in the Summary of Auditors' Results section of the accompanying Schedule of Findings and Questioned Costs.

Management's responsibility

Management is responsible for compliance with federal statutes, regulations, and the terms and conditions of its federal awards applicable to its federal programs.

Auditors' responsibility

Our responsibility is to express an opinion on compliance for each of the District's major federal programs based on our audit of the types of compliance requirements referred to above. We conducted our audit of compliance in accordance with U.S. generally accepted auditing standards; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and the audit requirements of Title 2 U.S. Code of Federal Regulations Part 200, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* (Uniform Guidance). Those standards and the Uniform Guidance require that we plan and perform the audit to obtain reasonable assurance about whether noncompliance with the types of compliance requirements referred to above that could have a direct and material effect on a major federal program occurred. An audit includes examining, on a test basis, evidence about the District's compliance with those requirements and performing such other procedures as we considered necessary in the circumstances.

We believe that our audit provides a reasonable basis for our opinion on compliance for each major federal program. However, our audit does not provide a legal determination of the District's compliance.

Opinion on each major federal program

In our opinion, Mohave County Community College District complied, in all material respects, with the types of compliance requirements referred to above that could have a direct and material effect on each of its major federal programs for the year ended June 30, 2016.

Report on internal control over compliance

The District's management is responsible for establishing and maintaining effective internal control over compliance with the types of compliance requirements referred to above. In planning and performing our audit of compliance, we considered the District's internal control over compliance with the types of requirements that could have a direct and material effect on each major federal program to determine the auditing procedures that are appropriate in the circumstances for the purpose of expressing an opinion on compliance for each major federal program and to test and report on internal control over compliance in accordance with the Uniform Guidance, but not for the purpose of expressing an opinion on the effectiveness of internal control over compliance. Accordingly, we do not express an opinion on the effectiveness of the District's internal control over compliance.

A deficiency in internal control over compliance exists when the design or operation of a control over compliance does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, noncompliance with a type of compliance requirement of a federal program on a timely basis. A material weakness in internal control over compliance is a deficiency, or a combination of deficiencies, in internal control over compliance, such that there is a reasonable possibility that material noncompliance with a type of compliance requirement of a federal program will not be prevented, or detected and corrected, on a timely basis. A significant deficiency in internal control over compliance is a deficiency, or a combination of deficiencies, in internal control over compliance with a type of compliance requirement of a federal program that is less severe than a material weakness in internal control over compliance, yet important enough to merit attention by those charged with governance.

Our consideration of internal control over compliance was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control over compliance that might be material weaknesses or significant deficiencies. We did not identify any deficiencies in internal control over compliance that we consider to be material weaknesses. However, material weaknesses may exist that have not been identified.

The purpose of this report on internal control over compliance is solely to describe the scope of our testing of internal control over compliance and the results of that testing based on the requirements of the Uniform Guidance. Accordingly, this report is not suitable for any other purpose.

Report on schedule of expenditures of federal awards required by the Uniform Guidance

We have audited the financial statements of the business-type activities and discretely presented component unit of Mohave County Community College District as of and for the year ended June 30, 2016, and the related notes to the financial statements, which collectively comprise the District's basic financial statements. We issued our report thereon dated January 19, 2017, that contained an unmodified opinion on those financial statements. Our report also included a reference to our reliance on other auditors. Our audit was conducted for the purpose of forming our opinions on the financial statements that collectively comprise the District's basic financial statements. The accompanying schedule of expenditures of federal awards is presented for purposes of additional analysis as required by the Uniform Guidance and is not a required part of the basic financial statements. Such information is the responsibility of the District's management and was derived from and relates directly to the underlying accounting and other records used to prepare the basic financial statements. The information has been subjected to the auditing procedures applied in the audit of the basic financial statements and certain additional procedures, including comparing and reconciling such information directly to the underlying accounting and other records used to prepare the basic financial statements or to the basic financial statements themselves, and other additional procedures in accordance with U.S. generally accepted auditing standards. In our opinion, the schedule of expenditures of federal awards is fairly stated in all material respects in relation to the basic financial statements as a whole.

Jay Zsorey, CPA
Financial Audit Director

March 20, 2017

ARIZONA
Auditor General
Making a Positive Difference

SCHEDULE OF FINDINGS AND QUESTIONED COSTS

Summary of auditors' results

Financial statements

Type of auditors' report issued on whether the financial statements audited were prepared in accordance with generally accepted accounting principles	Unmodified
Internal control over financial reporting	
Material weaknesses identified?	**Yes**
Significant deficiencies identified?	**Yes**
Noncompliance material to the financial statements noted?	**No**

Federal awards

Internal control over major programs	
Material weaknesses identified?	**No**
Significant deficiencies identified?	**None reported**
Type of auditors' report issued on compliance for major programs	Unmodified
Any audit findings disclosed that are required to be reported in accordance with 2 CFR 200.516(a)?	**No**

Identification of major programs

CFDA number	Name of federal program or cluster
84.007, 84.033, 84.063, 84.268	Student Financial Assistance Cluster

Dollar threshold used to distinguish between Type A and Type B programs	$750,000
Auditee qualified as low-risk auditee?	No

Other matters

Auditee’s Summary Schedule of Prior Audit Findings required to be reported in accordance with 2 CFR 200.511(b)?	Yes

Financial statement findings

2016-01

The District should establish procedures for preparing its annual financial report

Criteria—The District should have policies and procedures to help ensure that its annual financial report that includes its financial statements, note disclosures, required supplementary information, and other financial schedules is accurately compiled and prepared in accordance with U.S. generally accepted accounting principles (GAAP). Accurate financial statements prepared in accordance with GAAP provide valuable information to those charged with governance, management, and other financial statement users, to make important decisions about the District's financial operations.

Condition and context—The District's Governing Board and management depend on accurate financial statements to fulfill their oversight responsibilities and to report accurate information to the public and agencies from which the District receives funding. However, the District did not ensure that a detailed review of the District's annual financial report was performed by a reviewer who was knowledgeable of governmental accounting standards to help ensure the reported information's accuracy and propriety. As a result, the District's annual financial report contained misstatements and errors that required correction. For example, deferred outflows related to pensions, pension expenses, cash, accounts payable, accrued payroll, payroll expenses, and net position amounts were not accurately reported. Further, the deposits and investments, risk management, and discretely presented component unit notes contained errors or were incomplete.

Effect—Without a detailed review, the District's annual financial report could misstate amounts reported, omit important and required information, or contain other misstatements and errors. The District adjusted its financial statements, note disclosures, and required supplementary information, and other financial schedules to report the correct amounts and other required information.

Cause—The District lacked comprehensive written policies and procedures needed to accurately prepare and perform a thorough review of its annual financial report.

Recommendation—To help ensure that the District's annual financial report, including its financial statements, note disclosures, required supplementary information, and other financial schedules are accurate and prepared in accordance with GAAP, the District should develop and follow comprehensive written policies and procedures for compiling and presenting financial data within its annual financial report. The policies and procedures should include detailed instructions for compiling data from the District's accounting system and for obtaining information not readily available from the accounting system but necessary for financial statement preparation. The policies and procedures should require an employee, knowledgeable of GAAP and who did not prepare the annual financial report to perform a detailed review of it. The reviewer should make sure that the amounts are accurate and properly supported and the annual financial report is presented in accordance with GAAP.

The District's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

This finding is similar to prior-year finding 2015-01.

2016-02

The District should improve access controls over its information technology resources

Criteria—Logical access controls help to protect the district's information technology (IT) resources, which include its systems, network, infrastructure, and data, from unauthorized or inappropriate access or use, manipulation, damage, or loss. Logical access controls also help to ensure that authenticated users access only what they are authorized to. Therefore, the District should have effective internal control policies and procedures to control access to its IT resources.

Condition and context—The District did not have adequate policies and procedures or consistently follow its policies and procedures to help prevent or detect unauthorized or inappropriate access to its IT resources.

Effect—There is an increased risk that the District may not prevent or detect unauthorized or inappropriate access or use, manipulation, damage, or loss of its IT resources, including sensitive and confidential information.

Cause—The District lacked sufficient detailed instructions for employees to follow for granting and reviewing access to its IT resources.

Recommendation—To help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT resources, the District needs to develop and implement effective logical access policies and procedures over its IT resources. The information below provides guidance and best practices to help the District achieve this objective.

- **Review user access—**A periodic, comprehensive review should be performed of all existing employee accounts to help ensure that network and system access granted is needed and compatible with job responsibilities. Also, when an employee's job responsibilities change, a review of their access should be performed to ensure their access is compatible with the new job responsibilities.
- **Review and monitor key activity of users—**Key activities of users and those with elevated access should be reviewed for propriety.
- **Improve network and system password policies—**Network and system password policies should be improved and ensure they address all accounts.

The District's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

This finding is similar to prior-year finding 2015-02.

2016-03

The District should improve its risk-assessment process to include information technology security

Criteria—The District faces risks of reporting inaccurate financial information and exposing sensitive data. An effective internal control system should include a district-wide risk-assessment process that involves members of the District's administration and IT management to determine the risks the District faces as it seeks to achieve its objectives to report accurate financial information and protect sensitive data. An effective risk-assessment process provides the basis for developing appropriate risk responses and should include defining objectives to better identify risks and define risk tolerances; and identifying, analyzing, and responding to identified risks.

Condition and context—The District's risk-assessment process did not include a district-wide information technology (IT) security risk assessment over the District's IT resources, which include its systems, network, infrastructure, and data. Also, the District did not evaluate the impact disasters or other system interruptions could have on its critical IT resources.

Effect—There is an increased risk that the District's administration and IT management may not effectively identify, analyze, and respond to risks that may impact its IT resources.

Cause—The District did not have a documented process to perform risk assessment procedures that included IT security.

Recommendation—To help ensure the District has effective policies and procedures to identify, analyze, and respond to risks that may impact its IT resources, the District needs to implement a district-wide IT risk-assessment process. The information below provides guidance and best practices to help the District achieve this objective.

- **Conduct an IT risk-assessment process at least annually—**A risk-assessment process should include the identification of risk scenarios, including the scenarios' likelihood and magnitude; documentation and dissemination of results; review by appropriate personnel; and prioritization of risks identified for remediation. An IT risk assessment could also incorporate any unremediated threats identified as part of the district's security vulnerability scans.
- **Evaluate the impact disasters or other system interruptions could have on critical IT resources—**The evaluation should identify key business processes and prioritize the resumption of these functions within time frames acceptable to the entity in the event of contingency plan activation. Further, the results of the evaluation should be considered when updating its disaster recovery plan.

The District's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

This finding is similar to prior-year findings 2015-03 and 2015-05.

2016-04

The District should improve its contingency-planning procedures for its information technology resources

Criteria—It is critical that the District have contingency-planning procedures in place to provide for the continuity of operations and to help ensure that vital information technology (IT) resources, which include its systems, network, infrastructure, and data, can be recovered in the event of a disaster, system or equipment failure, or other interruption. Contingency planning procedures include having a comprehensive, up-to-date contingency plan; taking steps to facilitate activation of the plan; and having system and data backup policies and procedures.

Condition and context—The District's contingency plan lacked certain key elements related to restoring operations in the event of a disaster or other system interruption of its IT resources. In addition, the District did not perform regularly scheduled, comprehensive tests of its contingency plan, and it did not have documented policies and procedures for performing backups or testing them to ensure they were operational and could be used to restore its IT resources.

Effect—The District risks not being able to provide for the continuity of operations, recover vital IT systems and data, and conduct daily operations in the event of a disaster, system or equipment failure, or other interruption, which could cause inaccurate or incomplete system and data recovery.

Cause—The District has an outdated and incomplete contingency plan.

Recommendation—To help ensure district operations continue in the event of a disaster, system or equipment failure, or other interruption, the District needs to further develop its contingency planning procedures. The information below provides guidance and best practices to help the District achieve this objective.

- **Update the contingency plan and ensure it includes all required elements to restore operations—**Contingency plans should be updated at least annually for all critical information or when changes are made to IT resources, and updates to the plan should be communicated to key personnel. The plan should include essential business functions and associated contingency requirements, including recovery objectives and restoration priorities and metrics as determined in the entity's business-impact analysis; contingency roles and responsibilities and assigned individuals with contact information; identification of critical information assets and processes for migrating to the alternative processing site; processes for eventual system recovery and reconstitution to return the IT resources to a fully operational state and ensure all transactions have been recovered; and review and approval by appropriate personnel. The contingency plan should also be coordinated with incident-handling activities.
- **Move critical operations to a separate alternative site—**Policies and procedures should be developed and documented for migrating critical IT operations to a separate alternative site for essential business functions.
- **Test the contingency plan—**A process should be developed and documented to perform regularly scheduled tests of the contingency plan and document the tests performed and results. This process should include updating and testing the contingency plan at least annually or as changes necessitate, and coordinating testing with other plans of the entity such as its continuity of operations, cyber incident response, and emergency response plans. Plan testing may include actual tests, simulations, or table top discussions and should be comprehensive enough to evaluate whether the plan can be successfully carried out. The test results should be used to update or change the plan.

- **Train staff responsible for implementing the contingency plan**—An ongoing training schedule should be developed for staff responsible for implementing the plan that is specific to each user's assigned role and responsibilities.
- **Backup systems and data**—Establish and document policies and procedures for testing IT system software and data backups to help ensure they could be recovered if needed. Policies and procedures should require system software and data backups to be protected and stored in an alternative site with security equivalent to the primary storage site. Backups should include user-level information, system-level information, and system documentation, including security-related documentation.

The District's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

This finding is similar to prior-year finding 2015-03.

2016-05

The District should improve its configuration management processes over its information technology resources

Criteria—A well-defined configuration management process, including a change management process, is needed to ensure that the District's information technology (IT) resources, which include its systems, network, infrastructure, and data, are configured securely and that changes to these IT resources do not adversely affect security or operations. IT resources are typically constantly changing in response to new, enhanced, corrected, or updated hardware and software capabilities and new security threats. The District should have effective written configuration management internal control policies and procedures to track and document changes made to its IT resources.

Condition and context—The District's policies and procedures for managing changes to its IT resources lacked critical elements.

Effect—There is an increased risk that changes to the District's IT resources could be unauthorized or inappropriate or could have unintended results without proper documentation, authorization, review, testing, and approval prior to being applied.

Cause—The District's policies and procedures for managing changes to its IT resources were not fully implemented or reviewed to ensure they were in-line with current IT standards and best practices.

Recommendation—To help prevent and detect unauthorized, inappropriate, and unintended changes to its IT resources, the District needs to improve its policies and procedures over its configuration management processes. The information below provides guidance and best practices to help the District achieve this objective.

- **Establish and follow change management processes**—For changes to IT resources, a change management process should be established for each type of change, including emergency changes and other changes that might not follow the normal change management process. Further, all changes should follow the applicable change management process and should be appropriately documented.
- **Review proposed changes**—Proposed changes to IT resources should be reviewed for appropriateness and justification, including consideration of the change's security impact.

- **Document changes—**Changes made to IT resources should be logged and documented and a record should be retained of all change details, including a description of the change, the departments and system(s) impacted, the individual responsible for making the change, test procedures performed and the test results, security impact analysis results, change approvals at each appropriate phase of the change management process, and a post-change review.
- **Roll back changes—**Rollback procedures should be established that include documentation necessary to back out changes that negatively impact IT resources.
- **Test—**Changes should be tested prior to implementation, including performing a security impact analysis of the change.
- **Separate responsibilities for the change management process—**Responsibilities for developing and implementing changes to IT resources should be separated from the responsibilities of authorizing, reviewing, testing, and approving changes for implementation or, if impractical, performing a post-implementation review of the change to confirm the change followed the change management process and was implemented as approved.

The District's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

This is similar to prior-year finding 2015-04.

2016-06

The District should improve security over its information resources

Criteria—The selection and implementation of security controls for the District's information technology (IT) resources, which include its systems, network, infrastructure, and data, are important as they reduce the risks that arise from the loss of confidentiality, integrity, or availability of information that could adversely impact the District's operations or assets. Therefore, the District should implement internal control policies and procedures for an effective IT security process that include practices to help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT resources.

Condition and context—The District did not have sufficient written IT security policies and procedures over its IT resources.

Effect—There is an increased risk that the District may not prevent or detect the loss of confidentiality, integrity, or availability of systems and data.

Cause—The District's policies and procedures lacked critical elements related to IT security and the District did not adopt an IT standard and best practice framework to evaluate its policies and procedures against.

Recommendation—To help prevent, detect, and respond to instances of unauthorized or inappropriate access or use, manipulation, damage, or loss to its IT resources, the District needs to further develop its policies and procedures over IT security. The information below provides guidance and best practices to help the District achieve this objective.

- **Perform proactive logging and log monitoring**—Key user and system activity should be logged, particularly for users with administrative access privileges and remote access, along with other activities that could result in potential security incidents such as unauthorized or inappropriate access. An entity should determine what events to log and decide how often to monitor these logs for indicators of potential attacks or misuse of IT resources. Finally, activity logs should be maintained where users with administrative access privileges cannot alter them.
- **Prepare and implement an incident response plan—**An incident response plan should be developed, tested, and implemented for an entity's IT resources, and staff responsible for the plan should be trained. The plan should coordinate incident-handling activities with contingency-planning activities and incorporate lessons learned from ongoing incident handling in the incident response procedures. The incident response plan should be distributed to incident response personnel and updated as necessary. Security incidents should be reported to incident response personnel so they can be tracked and documented. Policies and procedures should also follow regulatory and statutory requirements, provide a mechanism for assisting users in handling and reporting security incidents, and making disclosures to affected individuals and appropriate authorities if an incident occurs.
- **Provide training on IT security risks—**A plan should be developed to provide continuous training on IT security risks, including a security awareness training program for all employees that provides a basic understanding of information security, user actions to maintain security, and how to recognize and report potential indicators of security threats, including threats employees generate. Security awareness training should be provided to new employees and on an ongoing basis.
- **Perform IT vulnerability scans—**A formal process should be developed for vulnerability scans that includes performing vulnerability scans of an entity's IT resources on a periodic basis and utilizing tools and techniques to automate parts of the process by using standards for software flaws and improper configuration, formatting procedures to test for the presence of vulnerabilities, measuring the impact of identified vulnerabilities, and approving privileged access while scanning systems containing highly sensitive data. In addition, vulnerability scan reports and results should be analyzed and legitimate vulnerabilities remediated as appropriate, and information obtained from the vulnerability-scanning process should be shared with other departments of the entity to help eliminate similar vulnerabilities.
- **Apply patches—**Patches to IT resources should be evaluated, tested, and applied in a timely manner once the vendor makes them available.
- **Implement IT standards and best practices—**IT policies and procedures should be reviewed against current IT standards and best practices, updated where needed, and implemented entity-wide, as appropriate. Further, staff should be trained on IT policies and procedures.

The District's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

This finding is similar to prior-year finding 2015-05.

2016-07

The District should improve its payroll policies and procedures

Criteria—The District should establish and maintain effective internal control policies and procedures to ensure employees are paid the correct amount and that employment agreements support payroll amounts.

Condition and context—The District did not have adequate internal control policies and procedures in place over payroll. Specifically, the District's review process over establishing beginning-of-the-year pay rate increases for input into the accounting system did not ensure that annual pay rate increases were accurate. For example, 4 of 91 employees tested were not paid in accordance with an approved agreement or the salary schedule, resulting in errors ranging from an $8,470 annual underpayment to a $365 annual overpayment. In addition, the District's review process did not require documentation of the review and approval of the schedule used to enter the pay rate increases into the accounting system.

Effect—The District did not pay all employees in accordance with approved pay rates. Additionally, there is a risk of fraud, theft, and abuse if expenditures are not properly supported, reviewed, and approved.

Cause—The District's review procedures were not effective to identify errors.

Recommendation—To help ensure that the District pays employees in accordance with agreed upon terms, the District should develop written policies and procedures for the independent review of annual pay rate increases entered into the accounting system. These procedures should require documentation of the review and approval of the schedule used to enter the pay rate increases into the accounting system.

The District's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

Federal award findings and questioned costs

None reported

DISTRICT SECTION

Mohave County Community College District
Schedule of expenditures of federal awards
Year ended June 30, 2016

Federal agency/CFDA number	Federal program name	Cluster title	Pass-through grantor	Pass-through grantor's number	Program expenditures
National Science Foundation					
47 076	Education and Human Resources				11,700
Small Business Administration					
59 037	Small Business Development Center		Maricopa County Community College District	SBAHQ-15-B-0040, SBAHQ-16-B-0051	71,834
Department of Education					
84 002	Adult Education—Basic Grants to States		Arizona Department of Education	16FAEAEF-612271-16B, 16FAEABE-612271-16B	104,327
84 007	Federal Supplemental Educational Opportunity Grants	Student Financial Assistance Cluster			102,562
84 033	Federal Work-Study Program	Student Financial Assistance Cluster			91,168
84 063	Federal Pell Grant Program	Student Financial Assistance Cluster			6,386,934
84 268	Federal Direct Student Loans	Student Financial Assistance Cluster			4,422,245
	Total Student Financial Assistance Cluster				11,002,909
84 048	Career and Technical Education—Basic Grants to States		Arizona Department of Education	15FCTDBG-512271-20A, 16FCTDBG-612271-20A	275,031
	Total Department of Education				11,382,267
	Total expenditures of federal awards				$ 11,465,801

See accompanying notes to schedule.

Mohave County Community College District
Notes to schedule of expenditures of federal awards
Year ended June 30, 2016

Note 1 - Basis of presentation

The accompanying schedule of expenditures of federal awards includes the federal grant activity of Mohave County Community College District for the year ended June 30, 2016. The information in this schedule is presented in accordance with the requirements of Title 2 U.S. Code of Federal Regulations (CFR) Part 200, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* (Uniform Guidance).

Note 2 - Summary of significant accounting policies

Expenditures reported on the Schedule are reported on the accrual basis of accounting. Such expenditures are recognized following the cost principles contained in the Uniform Guidance, wherein certain types of expenditures are not allowable or are limited as to reimbursement. Therefore, some amounts presented in this schedule may differ from amounts presented in, or used in the preparation of, the financial statements.

Note 3 - Catalog of Federal Domestic Assistance (CFDA) numbers

The program titles and CFDA numbers were obtained from the federal or pass-through grantor or the 2016 *Catalog of Federal Domestic Assistance*.

Note 4 - Indirect cost rate

The District did not elect to use the 10 percent de minimis indirect cost rate as covered in 2 CFR §200.414.

DISTRICT RESPONSE

MCC Mohave Community College

March 20, 2017

Debbie Davenport
Auditor General
2910 N. 44th St., Ste. 410
Phoenix, AZ 85018
Dear Ms. Davenport:

We have prepared the accompanying corrective action plan as required by the standards applicable to financial audits contained in *Government Auditing Standards* and by the audit requirements of Title 2 U.S. Code of Federal Regulations Part 200, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*. Specifically, for each finding we are providing you with the names of the contact people responsible for corrective action, the corrective action planned, and the anticipated completion date.

Sincerely,

Sonni Marbury, MBA, CFP ®
Dean of Business Services

Neal Campus - Kingman
1971 Jagerson Ave.
Kingman, AZ 86409
928.757.4331

Henry Campus - Bullhead City
3400 Highway 95
Bullhead City, AZ 86442
928.758.3926

Lake Havasu City Campus
1977 Acoma Blvd. West
Lake Havasu City, AZ 86403
928.855.7812

North Mohave Campus
480 S. Central
Colorado City, AZ 86021
928.875.2799
1.800.678.3992

www.mohave.edu
1.866.664.2836

MCC Mohave
Community
College

Mohave County Community College District
Corrective action plan
Year ended June 30, 2016

Financial statement findings

2016-01
The District should establish procedures to accurately record and report financial information

Sonni Marbury, Dean of Business
Anticipated completion date: April 30, 2017
The District accepts this finding. While the District has implemented previous recommendations of training other employees in financial reporting responsibilities and using a reviewer that was not involved in the financial statement preparation, extra resources have not been allocated to the business office for financial statement preparation. The District will request that additional resources are allocated in order to prioritize the preparation of the financial statements. The District will also formalize a documented procedure process of the financial statements.

2016-02
The District should improve access controls over its information technology resources

Mark Van Pelt, Executive Director of Information Technology
Anticipated completion date: October 21, 2016
The District accepts this finding. Initial steps have been taken to remediate each of the areas outlined in the finding. Written policies and procedures will be created to establish processes for allowing access to IT resources for new employees. This policy and procedure will include regular audits of user access to ensure that rights are in line with the employee's daily tasks. A best practice approach is being constructed and applied to server and network devices to ensure that adequate logging and monitoring takes place as a daily operation. Network and systems password policies have been changed to require complex, lengthy passwords to access District resources.

Neal Campus - Kingman
1971 Jagerson Ave.
Kingman, AZ 86409
928.757.4331

Henry Campus
- Bullhead City
3400 Highway 95
Bullhead City, AZ 86442
928.758.3926

Lake Havasu City Campus
1977 Acoma Blvd. West
Lake Havasu City, AZ 86403
928.855.7812

North Mohave Campus
480 S. Central
Colorado City, AZ 86021
928.875.2799
1.800.678.3992

www.mohave.edu
1.866.664.2836

MCC Mohave
Community
College

Mohave County Community College District
Corrective action plan
Year ended June 30, 2016

2016-03
The District should improve its risk-assessment process to include information technology security

Mark Van Pelt, Executive Director of Information Technology
Anticipated completion date: March 1, 2017
The District accepts this finding. Though the District has a robust risk assessment process, including regular meetings attended by key stakeholders and a well-defined process to add, modify, and approve initiatives, including review by the President's council and executive officers we will review the process and documentation and make any necessary changes. The District will formally document all information security risk-assessment procedures.

2016-04
The District should improve its contingency-planning procedures for its information technology resources

Mark Van Pelt, Executive Director of Information Technology
Anticipated completion date: March 1, 2017
The District accepts this finding and has begun revising the existing disaster recovery plan to include significant changes in the layout, support, and survivability of the current infrastructure. A policy to review the disaster recovery plan regularly has been implemented. Backup, restoration, triage, and contact trees will be updated and maintained as a part of this plan. Backup and disaster recovery testing will be implemented after finalization of the disaster recovery plan and tested regularly as a part of staff training. The District is preparing a project outline for a business impact analysis, to include loss of service, loss of personnel, and alternate communication plans in the event of a disaster.

Neal Campus - Kingman
1971 Jagerson Ave.
Kingman, AZ 86409
928.757.4331

Henry Campus
- Bullhead City
3400 Highway 95
Bullhead City, AZ 86442
928.758.3926

Lake Havasu City Campus
1977 Acoma Blvd. West
Lake Havasu City, AZ 86403
928.855.7812

North Mohave Campus
480 S. Central
Colorado City, AZ 86021
928.875.2799
1.800.678.3992

www.mohave.edu
1.866.664.2836

MCC Mohave Community College

Mohave County Community College District
Corrective action plan
Year ended June 30, 2016

2016-05
The District should improve its configuration management processes over its information technology resources

Mark Van Pelt, Executive Director of Information Technology
Anticipated completion date: March 22, 2017
The District accepts this finding, noting that change management for major systems was not in place until shortly before the June 30, 2016 year-end, and was not regularly reviewed. The District has change management software integrated into the current helpdesk system and is implementing a policy that will require changes to mission critical systems to be reviewed and approved by a change advisory board. The members of this board will consist of IT staff and key stakeholders for the affected systems.

2016-06
The District should improve security over its information resources

Mark Van Pelt, Executive Director of Information Technology
Anticipated completion date: March 1, 2017
The District accepts this finding. The District is continuously updating its disaster recovery plan. Elements of this plan rely on consistent protection of information technology resources. To this end the District is revising procedures and metrics for system logging on all server and network devices in the system. The District is creating a security response plan for security incidents and is identifying the personnel who will be involved in investigating, resolving, and documenting security incidents, should they occur. A training plan has been developed and is in place. The disaster recovery plan includes vulnerability scanning as part of testing the plan.

Neal Campus - Kingman
1971 Jagerson Ave.
Kingman, AZ 86409
928.757.4331

Henry Campus
- Bullhead City
3400 Highway 95
Bullhead City, AZ 86442
928.758.3926

Lake Havasu City Campus
1977 Acoma Blvd. West
Lake Havasu City, AZ 86403
928.855.7812

North Mohave Campus
480 S. Central
Colorado City, AZ 86021
928.875.2799
1.800.678.3992

www.mohave.edu
1.866.664.2836

MCC Mohave Community College

Mohave County Community College District
Corrective action plan
Year ended June 30, 2016

2016-07
The District should improve its payroll policies and procedures

Jennie Dixon, Director of Human Resources
Anticipated completion date: March 31, 2017
The District agrees with the need to develop written policies and procedures for an independent review of annual pay rate increases. The District will create a written document that outlines the processes currently in place as well as investigate areas for increased efficiency and accuracy.

Neal Campus - Kingman
1971 Jagerson Ave.
Kingman, AZ 86409
928.757.4331

Henry Campus
- Bullhead City
3400 Highway 95
Bullhead City, AZ 86442
928.758.3926

Lake Havasu City Campus
1977 Acoma Blvd. West
Lake Havasu City, AZ 86403
928.855.7812

North Mohave Campus
480 S. Central
Colorado City, AZ 86021
928.875.2799
1.800.678.3992

www.mohave.edu
1.866.664.2836

MCC Mohave Community College

March 20, 2017

Debbie Davenport
Auditor General
2910 N. 44th St., Ste. 410
Phoenix, AZ 85018
Dear Ms. Davenport:

We have prepared the accompanying summary schedule of prior audit findings as required by the audit requirements of Title 2 U.S. Code of Federal Regulations Part 200, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*. Specifically, we are reporting the status of audit findings included in the prior audit's schedule of findings and questioned costs. This schedule also includes the status of audit findings reported in the prior audit's summary schedule of prior audit findings that were not corrected.

Sincerely,

Sonni Marbury, MBA, CFP®
Dean of Business Services

Neal Campus - Kingman
1971 Jagerson Ave.
Kingman, AZ 86409
928.757.4331

Henry Campus - Bullhead City
3400 Highway 95
Bullhead City, AZ 86442
928.758.3926

Lake Havasu City Campus
1977 Acoma Blvd. West
Lake Havasu City, AZ 86403
928.855.7812

North Mohave Campus
480 S. Central
Colorado City, AZ 86021
928.875.2799
1.800.678.3992

www.mohave.edu
1.866.664.2836

MCC Mohave
Community
College

Mohave County Community College District
Summary schedule of prior audit findings
Year ended June 30, 2016

Status of Financial statement findings

The District should establish procedures to accurately record and report financial information

Finding no.: 2015-01
Status: Partially corrected

The District has revised the internal review process for financial statements and note disclosures by training more employees in review and preparation of the financial statements. In addition to the District incorporating financial statement review in to the Finance, Facilities, and Audit Committee, the District has put in place clear systems for review and version control. The roles and expectations of all personnel in year-end accounting processes have been clearly communicated. The District will continue in depth training of employees with financial aptitude in stages of financial statement preparation. The finding is only partially corrected, as the District absorbed another full-time position in the business office due to budget constraints. In the future, the District hopes to allocate more resources in order to incorporate recommendations further. Additionally, the District will formalize a written process for financial statement preparation.

The District should improve access controls over its information technology resources

Finding no.: 2015-02
Status: Partially corrected

Data center access is now controlled by badging personnel. A limited number of personnel are allowed access, and contractors or unbadged personnel must be escorted at all times. This policy is enforced both internally and externally by the hosting data center. Written policies and procedures will be created to establish processes for allowing access to IT resources for new employees as well as processes for terminating access to IT resources upon employee departure. This policy and procedure will include regular audits of user access to ensure that rights are in line with the employee’s daily tasks. Users currently do not have remote access rights to workstations, but do have access rights to virtual terminals.

Neal Campus - Kingman
1971 Jagerson Ave.
Kingman, AZ 86409
928.757.4331

Henry Campus
- Bullhead City
3400 Highway 95
Bullhead City, AZ 86442
928.758.3926

Lake Havasu City Campus
1977 Acoma Blvd. West
Lake Havasu City, AZ 86403
928.855.7812

North Mohave Campus
480 S. Central
Colorado City, AZ 86021
928.875.2799
1.800.678.3992

www.mohave.edu
1.866.664.2836

Mohave County Community College District
Summary schedule of prior audit findings
Year ended June 30, 2016

Policies and procedures for reviewing access rights to these terminals are part of the regular audit process. A best practice is applied to server and network devices to ensure that adequate logging and monitoring takes place as a daily operation. Network and systems password policies have been changed to require complex, lengthy passwords to access District resources. The finding was not fully corrected before the end of the June 30, 2016 year-end due to time limitations.

The District should improve its disaster recovery plan and data backup procedures for its information technology resources

Finding no.: 2015-03
Status: Not corrected

The District has begun revising the existing disaster recovery plan to include significant changes in the layout, support, and survivability of the current infrastructure. A policy to review the disaster recovery plan regularly has been implemented. Backup, restoration, triage, and contact trees will be updated and maintained as a part of this plan. Backup and disaster recovery testing will be implemented after finalization of the disaster recovery plan and tested regularly as a part of staff training. The District is preparing a project outline for a business impact analysis, to include loss of service, loss of personnel, and alternate communication plans in the event of a disaster. The finding was not fully corrected before the end of the June 30, 2016 year-end due to time limitations.

The District should improve its information technology change management processes

Finding no.: 2015-04
Status: Partially corrected

The District notes that change management for major systems was not in place until shortly before the June 30, 2016 year-end, and was not regularly reviewed. The District has change management software integrated into the current helpdesk system and requires change management tickets for all systems, permissions, or functional changes to software or systems, including upgrades and patching. The District will continue to review and enforce its change management process.

MCC Mohave Community College

Mohave County Community College District
Summary schedule of prior audit findings
Year ended June 30, 2016

The District should improve security over its information resources

Finding no.: 2015-05
Status: Partially corrected

The District is continuously updating its disaster recovery plan. Elements of this plan rely on consistent protection of information technology resources. To this end the District is revising procedures and metrics for system logging on all server and network devices in the system. The District has revised the Acceptable Use of Computing Resources policy include prohibitions against the installation of shareware, freeware, and non-work related software. The District is creating a security response plan for security incidents and is identifying the personnel who will be involved in investigating, resolving, and documenting security incidents, should they occur. Outdated software was identified and was upgraded or remediated by severely restricting access to the affected systems. A training plan has been developed and is in place. The disaster recovery plan includes vulnerability scanning as part of testing the plan. The District has revised the user agreement, which includes a social media component and will require the agreement to be signed by employees. The finding was not fully corrected before the end of the June 30, 2016 year-end due to time and resource limitations.

Neal Campus - Kingman
1971 Jagerson Ave.
Kingman, AZ 86409
928.757.4331

Henry Campus - Bullhead City
3400 Highway 95
Bullhead City, AZ 86442
928.758.3926

Lake Havasu City Campus
1977 Acoma Blvd. West
Lake Havasu City, AZ 86403
928.855.7812

North Mohave Campus
480 S. Central
Colorado City, AZ 86021
928.875.2799
1.800.678.3992

www.mohave.edu
1.866.664.2836

ARIZONA
Auditor General
Making a Positive Difference