A REPORT
TO THE
ARIZONA LEGISLATURE

Financial Audit Division

Single Audit

Mohave County Community College District

Year Ended June 30, 2015

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

Debra K. Davenport
Auditor General

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 of school districts, state agencies, and the programs they administer.

The Auditor General's reports are available at:

www.azauditor.gov

Printed copies of our reports may be requested by contacting us at:

Office of the Auditor General
2910 N. 44th Street, Suite 410 • Phoenix, AZ 85018 • (602) 553-0333

Mohave County Community College District
Single Audit Reporting Package
Year Ended June 30, 2015

Table of Contents

Report Issued Separately

Comprehensive Annual Financial Report

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, 2015, and the related notes to the financial statements, which collectively comprise the District's basic financial statements, and have issued our report thereon dated February 22, 2016. 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 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 deficiencies described in the accompanying Schedule of Findings and Questioned Costs as items 2015-02, 2015-03, 2015-04, and 2015-05 to be material weaknesses.

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 deficiency described in the accompanying Schedule of Findings and Questioned Costs as item 2015-01 to be a significant deficiency.

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 on pages 19 through 21. 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

March 7, 2016

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 OMB Circular A-133

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, 2015. 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 the requirements of laws, regulations, contracts, and grants 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 OMB Circular A-133, *Audits of States, Local Governments, and Non-Profit Organizations*. Those standards and OMB Circular A-133 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.

2910 NORTH 44th STREET • SUITE 410 • PHOENIX, ARIZONA 85018 • (602) 553-0333 • FAX (602) 553-0051

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, 2015.

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 OMB Circular A-133, 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.

Purpose of this Report

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 OMB Circular A-133. Accordingly, this report is not suitable for any other purpose.

Report on Schedule of Expenditures of Federal Awards Required by OMB Circular A-133

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, 2015, and the related notes to the financial statements, which collectively comprise the District's basic financial statements. We issued our report thereon dated February 22, 2016, 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 OMB Circular A-133 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 7, 2016

(This page is left intentionally blank)

Mohave County Community College District
Schedule of Expenditures of Federal Awards
Year Ended June 30, 2015

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				$ 19,217
Small Business Administration					
59 037	Small Business Development Centers		Maricopa County Community College District	SBAHQ-15-B-0040	70,490
Department of Education					
84 002	Adult Education—Basic Grants to States		AZ Department of Education	15FAEAEF-512271-16B, 15FAEABE-512271-16B	92,689
84 007	Federal Supplemental Educational Opportunity Grants	Student Financial Assistance Cluster			98,899
84 033	Federal Work-Study Program	Student Financial Assistance Cluster			105,072
84 063	Federal Pell Grant Program	Student Financial Assistance Cluster			7,530,333
84 268	Federal Direct Student Loans	Student Financial Assistance Cluster			5,843,110
	Total Student Financial Assistance Cluster				13,577,414
84 048	Career and Technical Education—Basic Grants to States		AZ Department of Education	14FCTDBG-470556-01A, 15FCTDBG-512271-20A	138,887
	Total Department of Education				13,808,990
	Total expenditures of federal awards				$ 13,898,697

See accompanying notes to schedule.

Mohave County Community College District
Notes to Schedule of Expenditures of Federal Awards
Year Ended June 30, 2015

Note 1 - Basis of Presentation

The accompanying Schedule of Expenditures of Federal Awards includes the federal grant activity of Mohave County Community College District and is presented on the accrual basis of accounting. The information in this schedule is presented in accordance with the requirements of OMB Circular A-133, *Audits of States, Local Governments, and Non-Profit Organizations*. Therefore, some amounts presented in the Schedule may differ from amounts presented in, or used in the preparation of, the financial statements.

Note 2 - Catalog of Federal Domestic Assistance (CFDA) Numbers

The program titles and CFDA numbers were obtained from the federal or pass-through grantor or the 2015 *Catalog of Federal Domestic Assistance.*

Note 3 - Subrecipients

The District did not provide federal awards to subrecipients during the year ended June 30, 2015.

Mohave County Community College District
Schedule of Findings and Questioned Costs
Year Ended June 30, 2015

Summary of Auditors' Results

Financial Statements

Type of auditors' report issued:	Unmodified	
	Yes	**No**
Internal control over financial reporting:		
Material weaknesses identified?	X	
Significant deficiencies identified?	X	
Noncompliance material to the financial statements noted?		X

Federal Awards

Internal control over major programs:		
Material weakness identified?		X
Significant deficiency identified?		X (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 Circular A-133 (section .510[a])?		X

Identification of major programs:

CFDA Number	Name of Federal Program or Cluster
	Student Financial Assistance Cluster:
84.007	Federal Supplemental Educational Opportunity Grants
84.033	Federal Work-Study Program
84.063	Federal Pell Grant Program
84.268	Federal Direct Student Loans

Mohave County Community College District
Schedule of Findings and Questioned Costs
Year Ended June 30, 2015

Dollar threshold used to distinguish between Type A and Type B programs:	$300,000

	Yes	No
Auditee qualified as low-risk auditee?	___	X

Other Matters

Auditee's Summary Schedule of Prior Audit Findings required to be reported in accordance with Circular A-133 (section .315[b])?	X	___

Mohave County Community College District
Schedule of Findings and Questioned Costs
Year Ended June 30, 2015

Financial Statement Findings

2015-01

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

Criteria: The District's internal controls should include policies and procedures to help ensure that it prepares an accurate and complete *Comprehensive Annual Financial Report* in accordance with generally accepted accounting principles.

Condition and context: The District's Governing Board and management depend on accurate information to fulfill their oversight responsibilities and to report accurate information to the public and agencies from which the District receives funding. Although the District implemented a review process during fiscal year 2014, the review process did not ensure that a detailed review of the District's *Comprehensive 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 financial statements, notes, and other reported information contained misstatements that ranged from mathematical errors and presentation errors to amounts not agreeing within the report and noncompliance with generally accepted accounting standards that required correction. For example, deferred outflows related to pensions and pension expenses were not accurately reported.

Effect: Without a detailed review, the District's financial statements could omit important and required information or contain other misstatements. The District adjusted its financial statements, notes, and other reported information within the *Comprehensive Annual Financial Report* to report the correct amounts and information.

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

Recommendation: To help ensure that the financial statements are accurate and prepared in accordance with generally accepted accounting principles, the District should:

- Develop and follow comprehensive written procedures for compiling and presenting financial data within the financial statements and accompanying notes; including detailed instructions for obtaining information not readily available from the accounting system, but necessary for financial statement preparation.
- Allocate the appropriate resources, and monitor and enforce completion dates for compiling, preparing, and reviewing the financial statements and supporting schedules.
- Train other employees in financial reporting responsibilities.
- Have an appropriate employee who did not prepare the financial statements review them and the accompanying notes. The reviewer should make sure that the amounts are accurate and properly supported and the financial statements are presented in accordance with generally accepted accounting principles.

This finding is similar to prior-year finding 2014-02.

2015-02

The District should improve access controls over its information technology resources

Criteria: The District should have effective internal control policies and procedures to control access to its information technology (IT) resources, which includes its systems, network, infrastructure, and data.

Condition and context: The District did not have written policies and procedures to control access to its IT resources. Specifically, the District did not have policies and procedures in place for granting, removing, limiting, and changing access to its IT resources, or to restrict physical access to its data center. Also, the District did not have policies and procedures in place for periodically reviewing employees' user account access to ensure their access remained necessary and appropriate. Auditors noted that the District allowed terminated employees access to its network and financial systems. In addition, the District did not have policies and procedures to periodically review remote access rights, which allows users to access network resources from locations other than district buildings. Further, the District did not have policies and procedures for logging and monitoring key activity on its network and systems. Finally, the District did not have effective policies and procedures for password protection for its network and systems.

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

Cause: The District has no one dedicated to ensuring policies and procedures are written and up to date.

Recommendation: To help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT resources, the District should establish and implement effective access control policies and procedures that include the following:

- Performing a periodic, comprehensive review of all existing employee access accounts to ensure that network and system access granted is needed and compatible with job responsibilities and remote access is appropriate when granted.
- Reviewing employees' network and systems access when their job responsibilities change to ensure access granted is compatible with their new job responsibilities.
- Removing employees' network and systems access immediately upon their termination.
- Restricting data center access to employees who need it for their job responsibilities and periodically reviewing access granted to ensure that it continues to be needed.
- Reviewing and monitoring the key activity of users and those with elevated access for propriety.
- Strengthening network and system password policies by increasing the password length, where applicable, and requiring employees to use complex passwords, change passwords on a periodic basis, and by developing a reasonable account lockout threshold for incorrect password attempts.

2015-03

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

Criteria: It is critical that the District have a comprehensive, up-to-date disaster recovery plan and data backup policies and procedures in place to provide for the continuity of operations and to help ensure that vital information technology (IT) resources, which includes its systems, network, infrastructure, and data, can be recovered in the event of a disaster, system or equipment failure, or other interruption.

Condition and context: The District did not have an adequate written disaster recovery plan. Auditors reviewed the District's disaster recovery processes and determined it lacked certain key elements for restoring operations, specifically:

- The plan lacked overall provisions for business continuity, including identifying essential mission and business functions and the associated requirements, maintaining essential functions despite an information system disruption, and communicating the plan to essential employees.
- The plan did not include an analysis and prioritization of recovery for key business processes, including acceptable time frames for restoring those processes.
- The plan did not reflect the current data backup process.
- The plan included contact names but did not provide contact information.
- The District did not have an alternate site should a disaster render the data center inoperable.
- The District did not keep its disaster recovery plan up to date.
- The District did not perform regularly scheduled, comprehensive tests of its plan; document test results; and update the plan for any problems noted.
- The District did not test its backup data, and it did not have written policies and procedures detailing the data backup procedures, including restoring the systems using the backup data in an emergency.
- The District did not communicate the disaster recovery plan to its staff.
- The District did not provide regular training of key personnel to ensure staff would be prepared to carry out the plan.

Effect: The District risks not being able to provide for the continuity of operations and recover vital IT resources 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 information and data and expensive recovery efforts.

Cause: The District has some processes in place but lacks a sufficiently documented recovery plan based on current IT standards and best practices to ensure that its disaster recovery efforts and backup data can be relied on in the event that they are needed.

Recommendation: To help ensure the continuity of the District's operations in the event of a disaster, system or equipment failure, or other interruption, the District should prepare a written disaster recovery plan that includes the following:

- Conduct a business impact analysis, including recovery objectives, restoration priorities, and metrics, into the disaster recovery plan to evaluate the impact that disasters could have on its critical business processes and revise its disaster recovery plan to include the analysis' results.
- Develop and document procedures for migrating critical information system operations to a separate alternative site for essential business functions. Contracts should be in place or the alternate site should be equipped to resume essential business functions, if necessary. Information security safeguards at the alternative site should be equivalent to the primary site.
- Ensure that its disaster recovery plan is updated for all critical information when changes are made to the IT resources and at least annually.
- Develop a process to perform regularly scheduled tests of the disaster recovery plan and document the tests performed and results. This process should include updating and testing the disaster recovery plan at least annually or as changes necessitate, and coordinate testing with other district plans such as its continuity of operation, 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. Use test results to update or change the plan.
- Establish and document policies and procedures for testing backups of IT systems and data to help ensure that the District could recover them in the event that they are needed. Policies and procedures should require 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. In addition, critical information system software and security-related information should be maintained at an alternative site or stored in a fire-rated container.
- Ensure the plan addresses how to communicate changes to key personnel.
- Develop and implement an ongoing training schedule for staff responsible for implementing the plan. In addition, ensure training provided is specific to the user's assigned roles and responsibilities.

2015-04

The District should improve its information technology change management processes

Criteria: The District should have adequate change management internal control policies and procedures to track and document changes made to its information technology (IT) resources, which includes its systems, network, infrastructure, and data.

Condition and context: The District did not have written policies and procedures for managing changes to its IT resources. Specifically, the District did not have a process for managing changes to its IT resources. For example, district changes to its IT resources were not documented, assessed for risk, prioritized, reviewed, approved, or tested. In addition, the District did not retain records of changes.

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 focused its efforts on the day-to-day operations and did not prioritize its IT change management policies and procedures.

Recommendation: To help prevent and detect unauthorized, inappropriate, and unintended changes to its IT resources, the District should establish written policies and procedures for change management that includes the following:

- Establishing a change management process for each type of change, including emergency changes and changes exempt from the change management process.
- Ensuring all changes follow its change management process and are appropriately documented.
- Reviewing proposed changes to determine appropriateness and justification, considering the security impact for the change.
- Logging, documenting, and retaining records of all change details, including test procedures, results, security impact analysis and approvals.
- Retaining necessary documentation to support the backing out of changes that negatively impact IT resources.
- Testing changes, including performing a security impact analysis before implementing the change.
- Separating the responsibilities for developing and implementing changes from the responsibilities of authoring, reviewing, testing, and approving changes for implementation.
- Approving the change at each appropriate phase of the change management process and documenting the approvals.
- Reviewing changes that were implemented to confirm they were implemented as approved and followed the change management process.

2015-05

The District should improve security over its information resources

Criteria: To effectively maintain and secure financial and sensitive information, the District should establish internal control policies and procedures that include practices to help prevent, detect, and respond to instances of unauthorized access or use, manipulation, damage, or loss to its information technology (IT) resources, which includes its systems, network, infrastructure, and data, that are based on acceptable IT industry practices.

Condition and context: The District did not have written policies to help secure its IT resources and did not adequately secure its IT resources. Specifically, the District did not:

- Develop a district-wide IT security risk-assessment process that is performed on a periodic basis or at least annually and includes identified risks, documentation of results, review by appropriate personnel, and prioritization of risks for remediation. In addition, any threats identified as part of the District's IT security vulnerability scans should be incorporated into the IT security risk assessment process.
- Have a policy to identify and classify data by sensitivity and take appropriate action to protect sensitive information. For example, auditors found that sensitive data was unsecured and potentially not restricted to only employees who required access to the information.

- Log and monitor key user and system activity.
- Require appropriate security measures, such as nonrooted phones, encryption, passwords, and remote wiping for employee-owned electronic devices with access to the District's network and monitor the use of these devices. For example, the District did not know what personal devices were accessing its IT resources.
- Manage the installation of software on employee workstations. For example, the District had no written policy or guidance to identify what software is appropriate, and there was no process to monitor and detect unauthorized software.
- Establish a process to respond to security incidents and provide training to those involved in the process.
- Establish a process to ensure IT resources have only essential services installed that the software requires to run.
- Assess the security risks associated with using outdated and unsupported software or take steps to secure the software. Specifically, the District was using outdated and unsupported software that may have been vulnerable because the vendor no longer provided security updates to protect against malicious attacks.
- Provide continuous training to keep IT personnel up to date on IT security risks, controls, and practices. In addition, the District did not have a security awareness program for its employees, nor did it have a training program to help ensure they were familiar with the District's IT security policies and procedures.
- Have a process to identify vulnerabilities in its IT resources on a periodic basis, nor did they have a plan to prioritize and remediate or mitigate identified vulnerabilities.
- Properly manage its IT vendors, such as providing guidance for procurement of IT vendor services that require consideration of IT risks, costs, benefits, and technical specifications; monitoring of vendors to ensure conformance with district contracts; and ensuring sensitive data is properly secured and protected.
- Have a process to test patches to ensure system functionality is not affected by recently released updates.
- The District did not have policies and procedures in place for electronic media protection to ensure sensitive information is handled appropriately when stored.
- The District did not have all employees sign the latest approved user agreement.
- The District did not have employees having access to the District's social media accounts sign an agreement that stipulates responsibilities and expected behavior regarding the use of those accounts.

Effect: There is an increased risk that the District may not prevent or detect unauthorized access or use, manipulation, damage, or loss to its IT resources.

Cause: The District was unaware its processes lacked critical elements related to IT security and did not evaluate its processes against current IT standards and best practices.

Recommendation: To help ensure that the District is able to effectively maintain and secure its IT resources, the District should prepare written policies and procedures that include the following:

- Conducting an IT security risk-assessment process when there are changes to the IT resources, or at least annually that includes identification of risk scenarios that could impact the District, including the scenarios' likelihood and magnitude; results' documentation and dissemination; review by appropriate personnel; and prioritization of risks for remediation. Also, incorporate any threats identified as part of the District's IT security vulnerability scans into the IT security risk-assessment process.
- Identifying, categorizing, and inventorying sensitive information and developing security measures to protect it, such as implementing controls to prevent unauthorized access to the information. In addition, the security categorizations, as well as the state statutes and federal regulations that impact the categorizations, should be documented as part of the District's policies and procedures.
- Performing proactive logging and log monitoring. The District should log key user and system activity, particularly users with administrative access privileges and remote access, along with other activities that could result in potential security incidents such as unauthorized access. The District should determine what events to log, configure the system to generate the logs, and decide how often to monitor these logs for indicators of potential attacks or misuse of IT resources. Also, the District should maintain activity logs where users with administrative access privileges cannot alter them.
- Managing employee-owned electronic devices connecting to the network, including specifying security configuration requirements; the data appropriate to access; inventorying devices; establishing controls to support wiping data; requiring security features, such as passwords, antivirus controls, and software updates; and restricting the running of unauthorized software applications while on the District's network.
- Managing software installed on employee computer workstations. Policies and procedures should address what software is appropriate and the process for requesting, approving, installing, monitoring, and removing software on employee computer workstations.
- Establishing and documenting a process to respond to security incidents. This process should include developing and testing an incident response plan and training staff responsible for the plan. The plan should define reportable incidents and address steps on how to handle incidents that includes preparation, detection and analysis, containment, eradication, and recovery. The plan should also 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 appropriate personnel and updated, as necessary. Suspected incidents should be reported to incident response personnel so incidents can be tracked and documented. The District should also ensure these policies and procedures follow regulatory and statutory requirements, provide a mechanism for assisting users in handling and reporting security incidents, and include making disclosures to affected individuals and appropriate authorities should an incident occur.
- Configuring IT resources to provide only essential capabilities to help prevent unauthorized connection of devices or transfer of information. The District should review IT resources' functions and services to determine which functions and services it should eliminate.
- Implementing a strategy for assessing and securing any software that the manufacturer no longer updates and supports.
- Developing a plan to provide continuous training on IT security risks, controls, and practices for the District's IT personnel. In addition, the District should develop a training program for all employees that provides a basic understanding of information security, user actions to maintain security, and instructions on how to recognize and report potential indicators of security threats, including threats other district employees generate. Provide such training for new users and on an ongoing basis as determined by the District.

- Developing a formal process for vulnerability scans that includes performing IT vulnerability scans 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, and measuring the impact of identified vulnerabilities. In addition, the District should analyze vulnerability scan reports and results, remediate legitimate vulnerabilities as appropriate, and share information obtained from the vulnerability-scanning process with district departments to help eliminate similar vulnerabilities.
- Developing and documenting a process to consider IT risks, costs, benefits, and technical specifications prior to awarding IT vendor contracts. In addition, the District should ensure contracts include specifications addressing the management, reliability, governance, and security of District IT resources. Finally, for cloud services, the District should ensure service contracts address all necessary security requirements based on best practices. The District should also monitor the IT vendor's performance to ensure conformance with district contracts.
- Developing patch-management policies and procedures to ensure patches are evaluated, tested, and applied in a timely manner once the vendor makes them available.
- Developing electronic media protection policies and procedures to restrict access to electronic media containing data the District, federal regulation, or state statute identifies as sensitive or restricted. Such policies and procedures should require that the District appropriately mark electronic media indicating the distribution limitations and handling caveats given the data included on the electronic media.
- Ensure that all employees sign the latest approved User Agreement.
- Ensure employees with access to the District's Social Media accounts sign an agreement acknowledging expected behavior and responsibilities.

Federal Award Findings and Questioned Costs

None reported.

MCC Mohave Community College

March 7, 2016

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 U.S. Office of Management and Budget Circular A-133. Specifically, for each financial reporting 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
Dean of Business

Mohave County Community College District Office
1971 Jagerson Ave.
Kingman, AZ 86409
928.757.4331

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

Distance Education Campus
1971 Jagerson Ave.
Kingman, AZ 86409
928.757.0867

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

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

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

www.mohave.edu
1.866.664.2832

Mohave County Community College District
Corrective Action Plan
Year Ended June 30, 2015

Financial Statement Findings

2015-01

The District should establish procedures to accurately record and report financial information
Contact person: Sonni Marbury, Dean of Business
Anticipated completion date: August 15, 2016

The District agrees that the internal review process for financial statements and note disclosures should be expanded to include training other employees in not only review, but preparation of the financial statements. Currently, the District has incorporated financial statement review in to the Finance, Facilities, and Audit Committee and although it has helped our internal review process, there are still areas to expand in education of employees that include internal involvement in not only review, but initial preparation of the statements. The District has already begun in depth training of employees with financial aptitude in stages of financial statement preparation. Written procedures in conjunction with training will alleviate this issue before the next fiscal year is at a close.

2015-02

The District should improve access controls over its information technology resources
Contact person: 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. 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. Policies and procedures for reviewing access rights to these terminals will created. 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.

Mohave County Community College District
Corrective Action Plan
Year Ended June 30, 2015

2015-03

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

Contact person: Mark Van Pelt, Executive Director of Information Technology

Anticipated completion date: October 21, 2016

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.

2015-04

The District should improve its information technology change management processes

Contact person: Mark Van Pelt, Executive Director of Information Technology

Anticipated completion date: December 31, 2016

The District accepts this finding, noting that change management for major systems was in place, but 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.

2015-05

The District should improve security over its information resources

Contact person: Mark Van Pelt, Executive Director of Information Technology

Anticipated completion date: December 31, 2016

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 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 is being identified and will be 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.

(This page is left intentionally blank)

MCC Mohave Community College

March 7, 2016

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 U.S. Office of Management and Budget Circular A-133. Specifically, we are reporting the status of audit findings included in the prior audit' s Schedule of Findings and Questioned Costs related to federal awards. 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
Dean of Business

Mohave County Community College District Office
1971 Jagerson Ave.
Kingman, AZ 86409
928.757.4331

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

Distance Education Campus
1971 Jagerson Ave.
Kingman, AZ 86409
928.757.0867

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

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

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

www.mohave.edu
1.866.664.2832

Mohave County Community College District
Summary Schedule of Prior Audit Findings
Year Ended June 30, 2015

Status of Federal Award Findings and Questioned Costs

CFDA No.: 84.031 **Higher Education—Institutional Aid**
Finding No.: 2013-101
Status: Fully corrected

CFDA No.: 84.031 **Higher Education—Institutional Aid**
Finding No.: 2014-101
Status: Fully corrected

CFDA No.: 84.031 **Higher Education—Institutional Aid**
Finding No.: 2014-102
Status: Fully corrected