Cochise County Community College District

Single Audit Report

Year Ended June 30, 2017

A Report to the Arizona Legislature

Debra K. Davenport
Auditor General

ARIZONA
Auditor General
Making a Positive Difference

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

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

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

Audit Staff

Jay Zsorey, Director
Victoria Fisher, Manager and Contact Person

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

District Section

District Response

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
Cochise County Community College District

We have audited the financial statements of the business-type activities and discretely presented component unit of Cochise County Community College District as of and for the year ended June 30, 2017, 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 30, 2018. Our report includes a reference to other auditors who audited the financial statements of the Cochise 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 Cochise 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 Cochise 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 have not been 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 2017-02, 2017-03, and 2017-04 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 deficiencies described in the accompanying schedule of findings and questioned costs as items 2017-01 and 2017-05 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*.

Cochise County Community College District's response to findings

Cochise County Community College District's responses to the findings identified in our audit are presented in its corrective action plan at the end of this 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 30, 2018

STATE OF ARIZONA

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

OFFICE OF THE
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
Cochise County Community College District

Report on compliance for each major federal program

We have audited Cochise 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, 2017. 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, Cochise 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, 2017.

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 Cochise County Community College District as of and for the year ended June 30, 2017, and the related notes to the financial statements, which collectively comprise the District's basic financial statements. We issued our report thereon dated January 30, 2018, that contained unmodified opinions 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 14, 2018

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
84.002	Adult Education—Basic Grants to States
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?	Yes

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

2017-01

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 an entity-wide risk-assessment process that involves members of the District's administration and information technology (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 annual risk-assessment process did not include a district-wide IT security risk assessment over the District's IT resources, which include its system, network, infrastructure, and data. Also, the District did not identify and classify sensitive information. Further, 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 lacked policies and procedures over risk-assessment and detailed instructions for employees to follow.

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 an entity's security vulnerability scans.
- **Identify, classify, inventory, and protect sensitive information—**Security measures should be developed to identify, classify, and inventory sensitive information and protect it, such as implementing controls to prevent unauthorized access to that information. Policies and procedures should include the security categories into which information should be classified, as well as any state statutes and federal regulations that could apply, and require disclosure to affected parties if sensitive information covered by state statutes or federal regulations is compromised.
- **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.

2017-02

The District should improve access controls over its information technology resources

Criteria—Logical and physical 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 written 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 adequate written policies and procedures and 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 effective logical and physical access policies and procedures over its IT resources. The District should review these policies and procedures against current IT standards and best practices and implement them district-wide, as appropriate. Further the District should train staff on the policies and procedures. 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.
- **Remove terminated employees' access to its IT resources—**Employees' network and system access should immediately be removed upon their terminations.
- **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.
- **Manage entity-owned electronic devices connecting to the network—**The use of entity-owned electronic devices connecting to the network should be managed, including specifying configuration requirements and the data appropriate to access; inventorying devices; establishing controls to support wiping data; requiring security features, such as passwords, antivirus controls, file encryption, and software updates; and restricting the running of unauthorized software applications while connected to the network.
- **Manage remote access—**Security controls should be utilized for all remote access. These controls should include appropriate configuration of security settings such as configuration/connections requirements and the use of encryption to protect the confidentiality and integrity of remote sessions.
- **Review data center access**—A periodic review of physical access granted to the data center should be performed to ensure that it continues to be needed.

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

2017-03

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 did not have policies and procedures for managing changes to its IT resources to ensure changes were properly documented, authorized, reviewed, tested, and approved. Also, the District did not have policies and procedures to ensure IT resources were configured securely.

Effect—There is an increased risk that the District's IT resources may not be configured appropriately and securely and that changes to those 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 lacked policies and procedures over configuration management and detailed instructions for employees to follow.

Recommendation—To help prevent and detect unauthorized, inappropriate, and unintended changes to its IT resources, the District needs to develop configuration management policies and procedures. The District should review these policies and procedures against current IT standards and best practices and implement them district-wide, as appropriate. Further, the District should train staff on the policies and procedures. 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 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.
- **Configure IT resources appropriately and securely and maintain configuration settings—**Configure IT resources appropriately and securely, which includes limiting the functionality to ensure only essential services are performed, and maintain configuration settings for all systems.
- **Manage software installed on employee computer workstations—**For software installed on employee computer workstations, policies and procedures should be developed to address what software is appropriate and the process for requesting, approving, installing, monitoring, and removing software on employee computer workstations.

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

2017-04

The District should improve security over its information technology 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 because 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 includes 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 written 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 lacked written policies and procedures for securing its IT resources.

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 develop its IT security policies and procedures. The District should review these policies and procedures against current IT standards and best practices and implement them district-wide, as appropriate. Further, the District should train staff on the policies and procedures. 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, 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. 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 its 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.
- **Protect sensitive or restricted data—**Restrict access to media containing data the entity, federal regulation, or state statute identifies as sensitive or restricted. Such media should be appropriately marked indicating the distribution limitations and handling criteria for data included on the media. In addition, media should be physically controlled and secured until it can be destroyed or sanitized using sanitization mechanisms with the strength and integrity consistent with the data's security classification.
- **Develop and document a process for awarding IT vendor contracts—**A process should be developed and documented to ensure the consideration of IT risks, costs, benefits, and technical specifications prior to awarding IT vendor contracts. In addition, contracts should include specifications addressing the management, reliability, governance, and security of the entity's IT resources. Further, for cloud services, ensure service contracts address all necessary security requirements based on best practices, such as physical location of data centers. Finally, an IT vendor's performance should be monitored to ensure conformance with vendor contracts.

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

2017-05

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. Also, although the District was performing system and data backups, it did not have documented policies and procedures for performing the 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 had an outdated plan that it is in the process of updating.

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 District should review its contingency planning procedures against current IT standards and best practices and implement them district-wide, as appropriate. 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 and stored in a secure location, accessible to those who need to use it and protected from unauthorized disclosure or modification.
- **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, including putting contracts in place or equipping the alternative site to resume essential business functions, if necessary. The alternative site's information security safeguards should be equivalent to the primary site.

- **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 tabletop 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. In addition, critical information system software and security-related information should be stored at an alternative site or in a fire-rated container.

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

Cochise County Community College District

Schedule of expenditures of federal awards

Year ended June 30, 2017

Federal agency/CFDA number	Federal program name	Cluster title	Pass-through grantor	Pass-through grantor's numbers	Program expenditures
Department of Agriculture					
10 U01 RBS-14-32	Rural Development-Cooperative Programs				$ 2,552
10 406	Farm Operating Loans				1,360
	Total Department of Agriculture				3,912
Department of Labor					
17 274	YouthBuild		Cochise County Private Industry Council	Youth Career Connect	11,526
Institute of Museum and Library Services					
45 129	Promotion of the Humanities—Federal/State Partnership		Arizona Humanities Council	70372016	4,274
45 310	Grants to States		Arizona State Library, Archives and Public Records	2015-0440-02	21,300
	Total Institute of Museum and Library Services				25,574
National Science Foundation					
47 076	Education and Human Resources				1,853
47 076	Education and Human Resources		Science Foundation Arizona	STEM 606-14/DUE-1400687	31,127
	Total 47.076				32,980
	Total National Science Foundation				32,980
Small Business Administration					
59 037	Small Business Development Centers		Maricopa County Community College District	6-603001-EZ-0026, SBHQ-17-B-0026	101,237
59 044	Veterans Outreach Program				206,922
	Total Small Business Administration				308,159
Department of Education					
84 002	Adult Education—Basic Grants to States		Arizona Department of Education	17FAEABE-712181-16B, 17FAEAPL-712181-16B, 17FAEADL-712181-16B, 17FAEIEL-712181-16B, 17FEDWIO-712181-16B	474,816
84 007	Federal Supplemental Educational Opportunity Grants	Student Financial Assistance Cluster			81,820
84 033	Federal Work-Study Program	Student Financial Assistance Cluster			91,895
84 063	Federal Pell Grant Program	Student Financial Assistance Cluster			6,249,965
84 268	Federal Direct Student Loans	Student Financial Assistance Cluster			1,622,712
	Total Student Financial Assistance Cluster				8,046,392

See accompanying notes to schedule.

Cochise County Community College District
Schedule of expenditures of federal awards
Year ended June 30, 2017

Federal agency/CFDA number	Federal program name	Cluster title	Pass-through grantor	Pass-through grantor's numbers	Program expenditures
84 042	TRIO—Student Support Services	TRIO Cluster			271,434
84 048	Career and Technical Education—Basic Grants to States		Arizona Department of Education	16FCTPSG-612181-43B, 16FCTDBG-612181-20A, 17FCTDBG-712181-20A	210,238
	Total Department of Education				9,002,880
	Total expenditures of federal awards				$ 9,385,031

See accompanying notes to schedule.

Cochise County Community College District
Notes to schedule of expenditures of federal awards
Year ended June 30, 2017

Note 1 - Basis of presentation

The accompanying schedule of expenditures of federal awards includes the federal grant activity of Cochise County Community College District for the year ended June 30, 2017. 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*.

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 2017 *Catalog of Federal Domestic Assistance*. When no CFDA number had been assigned to a program, the two-digit federal agency identifier and the federal contract number were used.

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 but rather used a negotiated rate per an agreement with the Department of Health and Human Services.

This page is intentionally left blank.

DISTRICT RESPONSE

COCHISE COLLEGE

901 North Colombo Avenue • Sierra Vista, AZ 85635-2317 • 520-515-0500 • www.cochise.edu

March 14, 2018

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,

LaMont Schiers
Vice President of Administrative Affairs

Financial statement findings

2017-01

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

Name(s) of contact person(s): Scott Clark
Anticipated completion date: March 31, 2019
District response: Concur

The District agrees with this recommendation and will implement the required policies and procedures to support an annual risk assessment plan. This assessment plan will aid the District in identifying risks, analyzing those risks, and determining the best course of action in addressing possible risks that could impact the District's information technology resources.

2017-02

The District should improve access controls over its information technology resources

Name(s) of contact person(s): Scott Clark
Anticipated completion date: August 31, 2018
District response: Concur

The District agrees with this recommendation and will implement policies and procedures and the required training to manage unauthorized access, misuse, damage or theft of its information technology resources; this initiative will follow IT industry standards and best practices.

2017-03

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

Name(s) of contact person(s): Scott Clark
Anticipated completion date: June 30, 2019
District response: Concur

The District agrees with this recommendation and will implement policies and procedures for configuration management. These policies and procedures will be based on IT industry standards and best practices in establishing the training, implementation and monitoring of the District's information technology resources as required.

Cochise County Community College District
Corrective action plan
Year ended June 30, 2017

2017-04

The District should improve security over its information technology resources
Name(s) of contact person(s): Scott Clark
Anticipated completion date: December 31, 2018
District response: Concur

The District agrees with this recommendation and will implement policies and procedures and the required training to manage unauthorized access, misuse, damage or theft of its information technology resources; this initiative will follow IT industry standards and best practices.

2017-05

The District should improve its contingency planning procedures for its information technology resources
Name(s) of contact person(s): Scott Clark
Anticipated completion date: June 30, 2019
District response: Concur

The District agrees with this recommendation and will implement policies and procedures to support a districtwide contingency plan that will be reviewed annually. These policies and procedures will be based on IT industry standards and best practices that will establish the training and regular review of this contingency plan.

COCHISE COLLEGE
901 North Colombo Avenue • Sierra Vista, AZ 85635-2317 • 520-515-0500 • www.cochise.edu

March 14, 2018

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,

LaMont Schiers
Vice President of Administrative Affairs

Cochise County Community College District
Summary schedule of prior audit findings
Year ended June 30, 2017

Status of financial statement findings

The District should improve security over its information technology resources

Finding number: 2016-01
Status: Not Corrected

The District continues to develop policies related to information technology resource security. The leadership and responsibly or our IT recourses has changed. The District has placed a high priority over this area and will continue to work towards full compliance with this recommendation.

Status of federal award findings and questioned costs

Cluster name: Student Financial Assistance Cluster
CFDA number and program name: 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; 93.925 Scholarships for Health Professions Students from Disadvantaged Backgrounds
Finding numbers: 2016-101, 2015-101, 2014-101
Status: Fully corrected

CFDA number and program name: 84.048 Career and Technical Education – Basic Grants to States
Finding number: 2016-102
Status: Fully corrected

ARIZONA
Auditor General
Making a Positive Difference