Yavapai County

Single Audit Report

Year Ended June 30, 2017

A Report to the Arizona Legislature

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 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

Report Issued Separately

Comprehensive annual financial report

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 Board of Supervisors of
Yavapai County, Arizona

We have audited, 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, the financial statements of the governmental activities, each major fund, and aggregate remaining fund information of Yavapai County as of and for the year ended June 30, 2017, and the related notes to the financial statements, which collectively comprise the County's basic financial statements, and have issued our report thereon dated December 20, 2017.

Internal control over financial reporting

In planning and performing our audit of the financial statements, we considered the County'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 County's internal control. Accordingly, we do not express an opinion on the effectiveness of the County'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 over financial reporting 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 County'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 County'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*.

Yavapai County response to findings

Yavapai County's responses to the findings identified in our audit are presented in its corrective action plan at the end of this report. The County'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 County'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 County's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Jay Zsorey, CPA
Financial Audit Director

December 20, 2017

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 Board of Supervisors of
Yavapai County, Arizona

Report on compliance for each major federal program

We have audited Yavapai County'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 County'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 County'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 County'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 County's compliance.

Opinion on each major federal program

In our opinion, Yavapai County 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 County'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 County'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 County'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 governmental activities, each major fund, and aggregate remaining fund information of Yavapai County as of and for the year ended June 30, 2017, and the related notes to the financial statements, which collectively comprise the County's basic financial statements. We issued our report thereon dated December 20, 2017, that contained unmodified opinions on those financial statements. Our audit was conducted for the purpose of forming our opinions on the financial statements that collectively comprise the County'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 County'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

February 13, 2018

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
10.665	Forest Service Schools and Roads Cluster
15.226	Payments in Lieu of Taxes
17.258, 17.259, 17.278	WIOA Cluster
20.106	Airport Improvement Program

Dollar threshold used to distinguish between Type A and Type B programs $750,000

Auditee qualified as low-risk auditee?   No

Other matters

Auditee's summary schedule of prior audit findings required to be reported in accordance with 2 CFR §200.511(b)?   Yes

Financial statement findings

2017-01
The County should improve its risk-assessment process to include information technology security

Criteria—The County 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 County's administration and IT management to determine the risks the County 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 County's annual risk-assessment process did not include a county-wide information technology (IT) security risk assessment over the County's IT resources, which include its systems, network, infrastructure, and data. Also, the County did not identify and classify sensitive information. Further, the County 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 County's administration and IT management may not effectively identify, analyze, and respond to risks that may impact its IT resources.

Cause—The County lacked policies and procedures over risk-assessment and detailed instructions for employees to follow.

Recommendation—To help ensure the County has effective policies and procedures to identify, analyze, and respond to risks that may impact its IT resources, the County needs to implement a county-wide IT risk-assessment process. The information below provides guidance and best practices to help the County 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 County's responsible officials' views and planned corrective action are in its corrective action plan at the end of this report.

2017-02
The County should improve access controls over its information technology resources

Criteria—Logical and physical access controls help to protect the County'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 County should have effective internal control policies and procedures to control access to its IT resources.

Condition and context—The County did not have 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 County 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 County lacked written policies and procedures for securing access to its IT resources.

Recommendation—To help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT resources, the County needs to develop effective logical and physical access policies and procedures over its IT resources. The County should review these policies and procedures against current IT standards and best practices and implement them county-wide, as appropriate. Further the County should train staff on the policies and procedures. The information below provides guidance and best practices to help the County 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 all shared accounts**—Shared network access accounts should be reviewed and eliminated or minimized when possible.
- **Manage shared accounts**—Shared accounts should be used only when appropriate and in accordance with an established policy authorizing the use of shared accounts. In addition, account credentials should be reissued on shared accounts when a group member leaves.
- **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 employee-owned and entity-owned electronic devices connecting to the network**—The use of employee-owned and 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.
- **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 County's responsible officials' views and planned corrective action are in its corrective action plan included at the end of this report.

2017-03

The County 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 County'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 County 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 County 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 County did not have policies and procedures to ensure IT resources were configured securely.

Effect—There is an increased risk that the County'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 County 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 County needs to develop configuration management policies and procedures. The County should review these policies and procedures against current IT standards and best practices and implement them county-wide, as appropriate. Further, the County should train staff on the policies and procedures. The information below provides guidance and best practices to help the County 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 systems 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 County's responsible officials' views and planned corrective action are in its corrective action plan at the end of this report.

2017-04
The County should improve security over its information technology resources

Criteria—The selection and implementation of security controls for the County'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 County's operations or assets. Therefore, the County 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 County did not have adequate written security policies and procedures over its IT resources.

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

Cause—The County lacked adequate 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 County needs to develop its IT security policies and procedures. The County should review these policies and procedures against current IT standards and best practices and implement them county-wide, as appropriate. Further, the County should train staff on the policies and procedures. The information below provides guidance and best practices to help the County 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 on going 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.

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

2017-05

The County should improve its contingency planning procedures for its information technology resources

Criteria—It is critical that the County 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 County'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 County 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 County 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 County has some processes in place but lacks a sufficiently documented contingency plan.

Recommendations—To help ensure county operations continue in the event of a disaster, system or equipment failure, or other interruption, the County needs to further develop its contingency planning procedures. The County should review its contingency planning procedures against current IT standards and best practices and implement them county-wide, as appropriate. The information below provides guidance and best practices to help the County 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 County's responsible officials' views and planned corrective action are in its corrective action plan at the end of this report.

This finding is similar to prior-year finding 2016-02.

Federal award findings and questioned costs

None reported.

Yavapai County
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	Amount provided to subrecipients
Department of Agriculture						
10 553	School Breakfast Program	Child Nutrition Cluster	Arizona Department of Education	ED09-0001	$ 18,340	
10 555	National School Lunch Program	Child Nutrition Cluster	Arizona Department of Education	ED09-0001	27,510	
10 555	National School Lunch Program (noncash)	Child Nutrition Cluster	Arizona Department of Education	ED09-0001	25,882	
	Total Child Nutrition Cluster				71,732	
10 557	Special Supplemental Nutrition Program for Women, Infants, and Children		Arizona Department of Health Services	ADHS14-053058	739,659	
10 561	State Administrative Matching Grants for the Supplemental Nutrition Assistance Program	SNAP Cluster	Arizona Department of Health Services	ADHS16-106460	198,191	
10 565	Commodity Supplemental Food Program	Food Distribution Cluster	Arizona Department of Health Services	ADHS17-132847	27,444	
10 578	WIC Grants To States (WGS)		Arizona Department of Health Services	ADHS14-053058	45,970	
10 665	Schools and Roads—Grants to States	Forest Service Schools and Roads Cluster			1,990,613	
10 U00 17-CS-11030900-015	Forest Service				74,572	
	Total Department of Agriculture				3,148,181	
Department of Housing And Urban Development						
14 228	Community Development Block Grants/State's program and Non-Entitlement Grants in Hawaii		Arizona Department of Housing	307-17	43,544	
Department of Interior						
15 226	Payments in Lieu of Taxes				3,314,664	
15 227	Distribution of Receipts to State and Local Governments				36,376	
	Total Department of Interior				3,351,040	
Department of Justice						
16 U01 2017-05	Domestic Cannabis Eradication/Suppression Program				7,690	
16 543	Missing Children's Assistance		Arizona Internet Crimes Against Children Task Force	2012-MC-FX-K008	5,000	
16 575	Crime Victim Assistance		Arizona Department of Public Safety	2015-291, 2015-464, 2015-481	252,798	
16 606	State Criminal Alien Assistance Program				49,537	
16 738	Edward Byrne Memorial Justice Assistance Grant Program				12,601	
16 738	Edward Byrne Memorial Justice Assistance Grant Program		Arizona Criminal Justice Commission	DC-17-011, DC-17-034	210,748	
	Total 16.738				223,349	
16 745	Criminal and Juvenile Justice and Mental Health Collaboration Program				6,000	
	Total Department of Justice				544,374	

Yavapai County
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	Amount provided to subrecipients
Department of Labor						
17 258	WIA/WIOA Adult Program	WIOA Cluster	Arizona Department of Economic Security	DI16-002118	437,837	$ 437,837
17 259	WIA/WIOA Youth Activities	WIOA Cluster	Arizona Department of Economic Security	DI16-002118	432,632	432,632
17 278	WIA/WIOA Dislocated Worker Formula Grants	WIOA Cluster	Arizona Department of Economic Security	DI16-002118	510,920	510,920
	Total WIA/WIOA Cluster				1,381,389	1,381,389
17 281	WIA/WIOA Dislocated Worker National Reserve Technical Assistance and Training		Arizona Department of Economic Security	DI16-002118	4,779	4,779
	Total Department of Labor				1,386,168	1,386,168
Department of Transportation						
20 106	Airport Improvement Program				544,838	
20 205	Highway Planning and Construction	Highway Planning and Construction Cluster	Arizona Department of Transportation	JPA 11-087	211,008	
20 505	Metropolitan Transportation Planning and State and Non-Metropolitan Planning and Research		Arizona Department of Transportation	JPA 11-087	67,748	
20 513	Enhanced Mobility of Seniors and Individuals with Disabilities	Transit Services Programs Cluster	Arizona Department of Transportation	JPA 11-087	36,901	
20 600	State and Community Highway Safety	Highway Safety Cluster	Arizona Governor's Office of Highway Safety	2016-AL-055, 2016-PS-016, 2016-PT-050, 2017-AL-053, 2017-CIOT-023, 2017-PS-012, 2017-PT-064	26,587	
20 616	National Priority Safety Programs	Highway Safety Cluster	Arizona Governor's Office of Highway Safety	2017-405d-039	10,250	
	Total Highway Safety Cluster				36,837	
	Total Department of Transportation				897,332	
Institute of Museum and Library Services						
45 310	Grants to States		Arizona State Library, Archives and Public Records	2016-36001-09	33,550	
Department of Education						
84 013	Title I State Agency Program for Neglected and Delinquent Children and Youth		Arizona Department of Education	17FLCCCL-713357-02A	8,630	
84 027	Special Education—Grants to States	Special Education Cluster (IDEA)	Arizona Department of Education	17FESCBG-710683-09A, 17FESCBG-713357-09A, 17FESSCG-710683-55, 17FESSCG-713357-55B, 17FESSLT-713357-01	245,039	
84 173	Special Education—Preschool Grants	Special Education Cluster (IDEA)	Arizona Department of Education	17FECCBP-713357-37A	13,195	
	Total Special Education Cluster (IDEA) Cluster				258,234	
84 365	English Language Acquisition State Grants		Arizona Department of Education	17FELENG-713357-66A	60,848	
84 367	Supporting Effective Instruction State Grant (formerly Improving Teacher Quality State Grants)		Arizona Department of Education	17FT1TII-713357-03A	9,747	
	Total Department of Education				337,459	

Yavapai County
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	Amount provided to subrecipients
Election Assistance Commission						
90 401	Help America Vote Act Requirements Payments		Arizona Secretary of State	None	19,432	
Department of Health and Human Services						
93 069	Public Health Emergency Preparedness		Arizona Department of Health Services	ADHS17-132201	314,531	
93 070	Environmental Public Health and Emergency Response		Arizona Department of Health Services	ADHS16-118059	5,474	
93 074	Hospital Preparedness Program (HPP) and Public Health Emergency Preparedness (PHEP) Aligned Cooperative Agreements		Arizona Department of Health Services	ADHS12-007898, ADHS17-133201	32,842	
93 136	Injury Prevention and Control Research and State and Community Based Programs		Arizona Department of Health Services	ADHS16-110838	106,845	
93 217	Family Planning—Services		Arizona Family Health Partnership	None	320,690	
93 224	Health Center Program (Community Health Centers, Migrant Health Centers, Health Care for the Homeless, and Public Housing Primary Care)	Health Center Program Cluster			477,654	
93 527	Grants for New and Expanded Services under the Health Center Program	Health Center Program Cluster			988,221	
	Total Health Center Program Cluster				1,465,875	
93 243	Substance Abuse and Mental Health Services—Projects of Regional and National Significance		Arizona Governor's Office of Youth, Faith and Family	PFS-GR-15-100115-03, PFS-GR-17-0931016-03	166,063	148,779
93 268	Immunization Cooperative Agreements		Arizona Department of Health Services	ADHS13-041551	13,362	
93 539	PPHF Capacity Building Assistance to Strengthen Public Health Immunization Infrastructure and Performance financed in part by Prevention and Public Health Funds		Arizona Department of Health Services	ADHS13-041551	169,858	
93 563	Child Support Enforcement		Arizona Department of Economic Security	G1304AZ4004	175,315	
93 597	Grants to States for Access and Visitation Programs		Arizona Department of Economic Security	1601AZSAVP	9,677	
93 752	Cancer Prevention and Control Programs for State, Territorial and Tribal Organizations financed in part by Prevention and Public Health Funds		Arizona Department of Health Services	ADHS14-064589	153,468	
93 757	State and Local Public Health Actions to Prevent Obesity, Diabetes, Heart Disease and Stroke (PPHF)		Arizona Department of Health Services	ADHS16-113864	71,000	
93 758	Preventive Health and Health Services Block Grant funded solely with Prevention and Public Health Funds (PPHF)		Arizona Department of Health Services	ADHS16-098338	63,132	
93 917	HIV Care Formula Grants		Arizona Department of Health Services	ADHS13-040485	77,317	
93 940	HIV Prevention Activities—Health Department Based		Arizona Department of Health Services	ADHS13-029720, ADHS17-165684	9,243	
93 959	Block Grants for Prevention and Treatment of Substance Abuse		Arizona Governor's Office of Youth, Faith and Family	IGA-SABG-GR-16-040116-14	55,034	
93 977	Preventive Health Services—Sexually Transmitted Diseases Control Grants		Arizona Department of Health Services	ADHS14-071220	9,426	

Yavapai County
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	Amount provided to subrecipients
93 994	Maternal and Child Health Services Block Grant to the States		Arizona Department of Health Services	ADHS14-074956, ADHS16-098338	273,076	
	Total Department of Health and Human Services				3,492,228	148,779

Corporation for National and Community Service
94 006	AmeriCorps		Arizona Supreme Court	None	562	

Department of Homeland Security
97 042	Emergency Management Performance Grants		Arizona Department of Emergency and Military Affairs	EMF-2016-EP-00009-S01	152,702	
97 045	Cooperating Technical Partners				449,674	
97 067	Homeland Security Grant Program		Arizona Department of Homeland Security	160517-01, 160517-02, 160518-01	58,912	
	Total Department of Homeland Security				661,288	
	Total expenditures of federal awards				$ 13,915,158	$ 1,534,947

Yavapai County
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 (schedule) includes Yavapai County's federal grant activity 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* (Uniform Guidance).

Note 2 - Summary of significant accounting policies

Expenditures reported on the schedule are reported on the modified 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 County did not elect to use the 10 percent de minimis indirect cost rate as covered in 2 CFR §200.414.

This page is intentionally left blank.

COUNTY RESPONSE

Yavapai County Finance Department

DANIEL RUSING, CPA   FINANCE DIRECTOR

February 1, 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 our responsible officials' views, the names of the contact people responsible for corrective action, the corrective action planned, and the anticipated completion date.

Sincerely,

Daniel Rusing
Finance Director

Yavapai County

Corrective action plan
Year ended June 30, 2017

Financial statement findings

2017-01

The County should improve its risk-assessment process to include information technology security
Name of contact person: Michael Holmes, MIS Director
Anticipated completion date: December 31, 2019
County response: Concur

In accordance with this finding MIS will perform a risk assessment on an annual basis within available time and financial limitations.

2017-02

The County should improve access controls over its information technology resources
Name of contact person: Michael Holmes, MIS Director
Anticipated completion date: December 31, 2019
County response: Concur

In accordance with the finding MIS will codify and formalize current practices into enhanced policies and procedures to help prevent or detect unauthorized or inappropriate access to its IT resources within available time and financial limitations.

2017-03

The County should improve its configuration management processes over its information technology resources
Name of contact person: Michael Holmes, MIS Director
Anticipated completion date: December 31, 2019
County response: Concur

In accordance with the finding MIS will codify and formalize current practices into enhanced policies and procedures to ensure that County IT resources are configured and installed properly within available time and financial limitations.

2017-04

The County should improve security over its information technology resources
Name of contact person: Michael Holmes, MIS Director
Anticipated completion date: December 31, 2019
County response: Concur

In accordance with the finding MIS will codify and formalize current practices into enhanced policies and procedures to ensure that proper access control to IT resources is maintained within available time and financial limitations.

Yavapai County
Corrective action plan
Year ended June 30, 2017

2017-05
The County should improve its contingency planning procedures for its information technology resources
Name of contact person: Michael Holmes, MIS Director
Anticipated completion date: December 31, 2019
County response: Concur

In accordance with the finding MIS will codify and formalize current practices into enhanced policies and procedures to ensure that continued operational access to County IT resources is maintained in the event of a disruption within available time and financial limitations.

Yavapai County Finance Department

DANIEL RUSING, CPA   FINANCE DIRECTOR

February 1, 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,

Daniel Rusing
Finance Director

Yavapai County
Summary schedule of prior audit findings
Year ended June 30, 2017

Status of financial statement findings

The County should establish policies and procedures for preparing its financial statements
Finding number: 2015-01, 2016-01
Status: Fully corrected

The County should improve its contingency planning procedures for its technology resources
Finding number: 2016-02
Status: Not corrected

MIS corrected all aspects of this finding except updating the contingency plan and training of all MIS related staff to restore operations due to staff turnover. Also, the second of the bi-annual "fail-over" tests that test both the secondary site and continuity of operation did not occur on schedule and will not occur till mid-February 2018 due to time and staffing resource availability from MIS, Finance, and Human Resources.