Financial Statement Findings and State Responses
(Reformatted from the FY 2015 Report on Internal Control and Compliance)

2015-01
The Arizona Department of Administration should prepare financial statements in a timely manner

Criteria: The Arizona Department of Administration (Department) should issue accurate and timely financial statements for the State of Arizona to satisfy the audit requirements imposed by federal and state laws and regulations, grants, contracts, and long-term debt agreements.

Condition and context: The Director of the Department is responsible for establishing and maintaining the State's accounting systems and preparing accurate and timely financial reports, including the State's *Comprehensive Annual Financial Report (CAFR)*. In accordance with Arizona Revised Statutes (A.R.S.) §41-703, the Director has the authority to promulgate rules, regulations, and procedures to carry out his responsibilities. Further, A.R.S. §35-131(I) requires state agencies and other organizations included in the State's reporting entity to submit all necessary financial statements or information to the Department to be used in preparing the State's CAFR. However, those statutes did not include provisions to enforce compliance, and as a result, state agencies did not always comply with the established deadlines. The Department had a deadline of November 2015 for the receipt of audited financial statements in order to issue the State's CAFR by December 31, 2015. Specifically, 14 state agencies had a November 2015 deadline to submit their audited financial statements, however, only 9 met this deadline and the Arizona Department of Transportation (ADOT) did not submit its audited financial statements until April 22, 2016.

Effect: Since various state agencies did not submit all necessary financial statements or financial information to the Department in a timely manner, the Department was unable to prepare and issue the State's CAFR by its December 31, 2015 deadline. Delays in financial reporting may result in rating agencies lowering the State's ratings for bonds and certificates of participation. Also, the State's Single Audit Reporting Package will be issued late (see finding 2015-101), which could result in a loss of federal funding.

Cause: State statutes do not provide the Director of the Department with enforcement power to ensure that state agencies comply with department rules, regulations, and procedures for financial reporting. Further, see findings 2015-12 and 2015-13 for additional detail regarding ADOT's late submission.

Recommendation: To help ensure that the Department receives all financial information necessary to prepare and issue the State's CAFR in a timely manner, the Department should:

- Seek the authority to enforce rules, regulations, and procedures over financial reporting.
- Establish enforcement actions for agencies' failure to submit such information by the required deadlines.

This finding is also reported as a federal finding. See finding 2015-101.

Agency Response: Concur

The Arizona Department of Administration
Name of contact person and title: Clark Partridge, State Comptroller
Anticipated completion date: 2018

The FY15 State of Arizona Comprehensive Annual Financial Report (CAFR) was impeded due to the delay of receipt of the financial statements for the Arizona Department of Transportation (ADOT). The ADOT financial statements are a significant portion of the State's financial activity. The delay is the result of complete turnover in ADOT's staff producing the agency's financial statements and the limited availability of other resources to assist due to the implementation of the State's new accounting system. The CAFR has been accurately prepared. Timeliness is the issue, and is one of the fundamental thresholds of financial reporting. Timely issue of the CAFR is vital to other

reporting requirements and deadlines. Arizona Revised Statutes (A.R.S.) §35-131 clearly requires State agencies and other organizations that are part of the State's reporting entity to submit all necessary financial statements and other information in accordance with the policies and procedures of the Arizona Department of Administration, General Accounting Office. This includes adherence to the established time frames and deadlines. However, there are no specific provisions in the law for actions that may be taken to enforce such compliance. We can continue to explore potential options for enforcement actions and will continue to work with State agencies to effectively resolve the issue of timely submission of financial information.

2015-02
The State of Arizona should strengthen its internal control policies and procedures and system controls over its ProcureAZ purchasing system.

Criteria: ProcureAZ is the State's Web-based procurement and purchasing system. Therefore, the State should have effective internal control policies and procedures and system controls over the ProcureAZ system. In addition, the State should monitor that those controls are in place and are being followed.

Condition and context: The State did not have effective internal control policies and procedures and system controls over its ProcureAZ system. As a result, auditors noted the following:

- The user roles established in the system did not appropriately separate duties. For example, a user can both enter and approve a purchase requisition and/or purchase order, and further, receive the goods ordered. Also, a user can enter an invoice in the system and approve it for payment.

- The document approval process in the system for each agency was not always set up properly. Several agencies did not establish adequate approval levels in the system to ensure all transactions received the appropriate level of review and approval.

- There was limited training required for state agencies that requested or established their own user access. As a result, agencies may not fully understand their responsibilities for granting user access to ensure that the user roles did not conflict with existing access or ensure appropriate separation of duties.

- There was no formal policy or procedures in place to ensure user access was removed for terminated employees by the State Procurement Office (SPO) and state agencies.

- The ProcureAZ system lacked reports and audit logs to allow the state agencies and the SPO to monitor user access and activity in the system. Without these reports, individual agencies and the SPO were unable to identify user access or activity in the system that may be inappropriate and should be investigated.

Effect: The State may have an increased risk of misuse, waste, theft of public monies, and unauthorized purchases.

Cause: The State did not have sufficient internal control policies and procedures, system controls, lacked detailed training to properly assign user roles and approval levels, and remove user access for terminated employees. In addition, the ProcureAZ system did not have sufficient reporting tools or audit logs to generate the information needed to monitor user access and activity within the system.

Recommendation: To help improve internal controls over the State's ProcureAZ system, the State should develop and implement internal control policies and procedures, establish system controls, and provide trainings to help ensure duties are appropriately separated, transactions are properly reviewed and approved, and terminated employees' access is removed from the system. Specifically, the State and its agencies should perform a comprehensive review to ensure employees' access and the user roles granted is needed and compatible with their job responsibilities, and correct any incompatible duties identified. Further, the State should develop reports and audit logs within the system to assist with monitoring user access and activity. Lastly, the State should

implement monitoring and oversight procedures to help ensure state agencies have properly implemented the State's ProcureAZ system's policies and procedures.

Agency Response: Concur

Name(s) of contact person(s): Clark Partridge, State Comptroller; and Judy Wente, State Procurement Office Assistant Director
Anticipated completion date: 2018

The State has already addressed some of these issues and will continue to identify and pursue appropriate corrective actions. The State has an audit report (GAO Security User Audit Report) to monitor the creation and approval of invoices in ProcureAZ. This report identifies the creator and final approver for each invoice and is available to all users with the appropriate reporting role in ProcureAZ. The State is also in the process of creating two audit reports that will provide assistance in monitoring purchase requesters and purchase approvers. Once approved, these reports will be available to all users with the appropriate reporting role in ProcureAZ. The State also plans to staff the position responsible for defining e-procurement system policies and procedures.

2015-03
The Department of Administration should improve security over its information technology resources

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

Condition and context: The Department did not:

- Identify and categorize data by sensitivity and take appropriate action to protect sensitive information.
- Develop and implement a Department-wide IT security risk assessment process.
- Have policies and procedures or a process in place to ensure its IT resources were configured securely.
- Log and monitor key user and system activity.
- Have a process to ensure compliance with its IT policies and procedures Department-wide including monitoring and reporting on non-compliance issues.

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

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

Recommendation: To help ensure the Department is able to effectively maintain and secure its IT resources the Department should ensure that its policies and procedures over securing its IT resources are reviewed against current IT standards and best practices, updated where needed, approved, and communicated Department-wide, as appropriate. The policies and procedures should be monitored for compliance and include the following:

- Identifying, categorizing, and inventorying sensitive information and developing security measures to protect it, such as implementing controls to prevent unauthorized access to the information. The Department's policies and procedures should include the security categories into which information should be classified as well as the state statutes and federal regulations that impact those categories.
- Conducting an IT security risk assessment process, when there are changes to the IT resources or at least annually, that includes identification of risk scenarios that could impact the Department, including the

scenarios' likelihood and magnitude, documentation and dissemination of results, review by appropriate personnel, and prioritization of risks for remediation. Also incorporate any threats identified as part of the Department's IT security vulnerability scans into the IT security risk assessment process.

- Developing and implementing policies and procedures for configuration management. Such policies and procedures should ensure the Department configures its IT resources to provide only essential capabilities to help prevent unauthorized connection of devices or transfer of information. Additionally, the Department should review IT resources' functions and services to determine which functions and services it should eliminate.
- Performing proactive logging and monitoring. The Department should log key user and system activity that could result in potential security incidents such as unauthorized access. The Department should determine what events to log, configure the system to generate the logs, and decide how often to monitor these logs for indicators of potential attacks or misuse of IT resources. Also, the Department should maintain activity logs where users with administrative access privileges cannot alter them.
- Establishing and implementing a formal security compliance policy and process, which consists of obtaining regular confirmation of compliance from process owners, ensuring that internal and external compliance reviews are performed against internal policies, and implementing a process to monitor and report on non-compliance issues. As a component of their compliance policy, the Department should include an enforcement mechanism to ensure that policies are effective and being followed.

Agency Response: Concur

Name of contact person and title: Darrell, Davis, Chief Privacy Officer
Anticipated completion date: December 31, 2016

The Department of Administration (ADOA) has recently begun implementing a Security Information and Event Management service and an Enterprise Directory Services solution that will be implemented throughout the Executive Branch agencies. These solutions will provide the Executive Branch Agencies with the increased abilities to identify their assets, perform risk-assessments, ensure policy compliance, log and monitor key activity and identify non-compliance. Both of these solutions are enterprise class solutions and ADOA is a pilot agency. ADOA anticipates these solutions will be fully implemented within our department by December 31, 2016.

2015-04
The Department of Administration should improve access controls over its information technology resources

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

Condition and context: The Department did not have adequate policies and procedures to control access to its IT resources. Specifically, the Department did not:

- Ensure all user accounts are uniquely identifiable and assigned to an individual employee.
- Periodically review user access to ensure access remained necessary and appropriate.
- Ensure generic user accounts are appropriately limited.
- Ensure compliance with its Access Control Policy by removing user accounts for terminated employees.

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

Cause: The Department focused its efforts on the day-to-day operations and did not prioritize its review of IT policies and procedures or assess against IT best practices.

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

- Performing a periodic, comprehensive review of all existing employee access accounts to ensure network and system access granted is unique to each employee, needed, and compatible with job responsibilities.
- Reviewing all generic and administrator accounts to eliminate or minimize their use where possible.
- Removing employees' access immediately upon their termination.

Agency Response: Concur

Name of contact person and title: Darrell Davis, Chief Privacy Officer
Anticipated completion date: May 31, 2017

The Department of Administration has recently begun implementing a Security Information and Event Management service and an Enterprise Directory Services solution that will be implemented throughout the Executive Branch agencies. These solutions will provide the Executive Branch Agencies with increased abilities to ensure proper identification and authorization for all user accounts and access. They will also provide a more mature monitoring, reporting, auditing, logging and compliance. We anticipate that ADOA will have these solutions fully implemented and the new processes documented within our department by May 31, 2017.

2015-05
The Arizona Department of Administration's Data Center should strengthen their contracts with state agencies

Criteria: Information technology (IT) services that the Arizona Department of Administration's Data Center (Data Center) provides to state agencies should be well documented, complete, comprehensive, up to date, and include all parties' responsibilities. Well-documented and up-to-date services provide staff with repeatable processes and clear expectations. In addition, the Data Center should maintain a listing of state agencies it has provided services to and the services provided.

Condition and context: The Data Center's IT service contracts with state agencies are broad, not agency specific, and do not adequately address critical services, including disaster recovery. Consequently, agencies may not understand their responsibilities in the event of a disaster, including what they would need to provide (e.g., data, software, etc.) to the Data Center.

Effect: Current contracts for services between the Data Center and state agencies could result in the failure to clearly communicate policies and procedures, limit staff accountability, and result in inconsistencies. For example, if a major disruption or disaster were to occur, the order in which systems were restored may not match individual state agencies' or the State's criticality or operational priorities. In addition, state agencies might incorrectly assume that the Data Center will always provide full off-site backup and disaster recovery.

Cause: The Data Center did not have sufficient policies and procedures to help ensure their contracts with state agencies, including disaster recovery services, are specific for each state agency and are updated as needed. In addition, the Data Center did not maintain a comprehensive listing of state agencies it provided services to along with the services provided.

Recommendation: To help ensure IT service Contracts between the Data Center and state agencies are complete and up to date, the Data Center should strengthen its IT services policies and procedures. The procedures dshould include establishing a comprehensive listing of the state agencies' systems maintained and clarifying the specific roles and responsibilities that all parties play in disaster recovery efforts. Further, the Data Center should ensure that the services provided are appropriately identified on the, listing, state agency systems are prioritized for recovery based on their relative importance, and the listing is updated as the needs of the state agency changes.

The information from the listing should also be included in the IT service contact with each state agency and provided either in summary form or a contract revision to each state agency.

This finding is similar to prior-year finding 2014-01.

Agency Response: Concur

Name of contact person and title: Darrell Davis, Chief Privacy Officer
Anticipated completion date: June 30, 2017

ADOA will develop agency specific language within our inter-agency agreements for the specific services we deliver and what specific services we do not deliver, to include disaster recovery, for each agency. We will also work with the agencies to get them executed. ADOA anticipates we can have these new agreements created and delivered to the agencies by June 30, 2017.

2015-06
The State of Arizona should strengthen its internal controls over purchasing cards

Criteria: The State's General Accounting Office (GAO) Technical Bulletin 08-1, *Statewide Purchasing Card (P-Card) Policies and Procedures*, requires state agencies to establish policies, procedures, and documentation requirements for p-card transactions that conform to the State's policies and procedures. In addition, this technical bulletin requires agencies to restrict the use of the p-cards to acquiring or paying for goods and services that will be used for a valid public purpose. Further, Attorney General Opinion I10-003 directs that the expenditure of public monies must be for a public purpose in which the expenditure does not exceed the worth of the direct benefits enjoyed by the public body.

Condition and context: The Department of Health Services used p-cards to purchase gift cards and gifts for patients of the Arizona State Hospital during the month of December 2014. The Department indicated the gift cards were purchased to be used as rewards for patient behavior; however, it was unable to provide evidence that the cards given to the patients were used for that purpose or demonstrate the public purpose of the gifts.

Effect: The State may have an increased risk of misuse, waste, or theft of public monies related to p-card transactions.

Cause: The State relies on the individual state agencies' management to implement their own p-card policies and procedures that conform to the State's p-card policies and procedures. However, the State does not ensure the agencies have implemented policies and procedures and does not always monitor compliance with established policies and procedures.

Recommendation: To help prevent and detect potential fraud, waste, and abuse related to p-card transactions, the GAO should establish monitoring and oversight procedures to help ensure that individual state agencies have properly developed and implemented p-card policies and procedures, as directed by the GAO's *Statewide Purchasing Card (P-Card) Policies and Procedures* and Attorney General Opinion I10-003.

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

Agency Response: Concur

Name of contact person and title: Clark Partridge, State Comptroller
Anticipated completion date: June 30, 2016

The State understands the importance of internal controls over purchasing cards. We will continue to review and update monitoring and oversight procedures as appropriate, as well as work with State agencies to ensure compliance with established policies.

The Department of Health Services has instituted procedures that require documentation be maintained with the Controller's Office identifying patients that receive gift cards as a reward for appropriate behavior and are used as therapy for community reintegration. The documentation will be in either hardcopy or electronic form and will now include the doctor's order for the reward. All supporting documentation will be maintained as part of the agency's records for five years past the end of the fiscal year of the purchase.

2015-07
The State of Arizona should strengthen its conflict of interest practices

Criteria: Arizona Revised Statutes (A.R.S.) §38-503 regarding conflicts of interest states that any public officer or employee of a state agency who has, or whose relative has, a substantial interest in any contract, sale, purchase, or service to that particular public agency shall make known that interest in that state agency's official records and shall refrain from voting upon or otherwise participating in any manner as an officer or employee in such contract, sale, or purchase. Further, financial accounting standards require that financial statements include disclosures of significant related-party transactions. To comply with these requirements, the State's General Accounting Office (GAO) issued Technical Bulletin No. 09-6, which requires all members of management to file an Annual Declaration and Disclosure form with their agency. The agency must file the form even if there are no conflicts noted and maintain the form for administrative and audit purposes. In addition, state agencies must complete and submit to the GAO Form 51 each year if the agency has any related-party transactions that aggregate to $100,000 or more for financial statement reporting purposes.

Condition and context: Several state agencies did not have controls in place to ensure that employees in management positions completed an annual conflict-of-interest declaration and, as a result, the agencies could not determine if there were any conflicts of interest or related-party transactions.

Effect: There is a risk that a conflict of interest may exist and related-party transactions were not reported to GAO for disclosure in the State's financial statements. Further, expenditures may have occurred that resulted in employee personal gain or were otherwise inappropriate.

Cause: The agencies were not aware that all employees in management positions must complete a conflict-of-interest declaration annually.

Recommendation: The Department should ensure that all management employees complete a conflict-of-interest Annual Declaration and Disclosure form to help ensure compliance with A.R.S. §38-503 and GAO's Technical Bulletin No. 09-6. In addition, when conflicts of interest exist, those employees with a conflict must refrain from voting upon or otherwise participating in any manner as an officer or employee in such contract, sale, or purchase. Further, if an agency has related-party transactions that aggregate to $100,000 or more, they should be reported to GAO for disclosure in the State's financial statements.

Agency Response: Concur

Name of contact person and title: Clark Partridge, State Comptroller
Anticipated completion date: June 30, 2017

We will review the conflict of interest statute and policy, along with the related compliance, and determine appropriate actions.

2015-08
The Department of Revenue should improve access controls over its information technology resources

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

Condition and context: The Department drafted new written policies in May 2015; however, these policies had not been fully implemented. As a result, the Department did not periodically perform reviews of user access, group accounts, or logs to:

- Restrict access to sensitive files and information on the network.
- Remove access rights for terminated employees and unused user accounts.
- Eliminate administrator access assigned to standard accounts.
- Ensure that all passwords are changed on a periodic basis.

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

Cause: The Department's new policies have not been fully implemented.

Recommendation: To help prevent and detect unauthorized access or use, manipulation, damage, or loss to its IT resources, the Department should implement its new policies and procedures over management of access controls across its IT resources that include the following:

- Performing a periodic, comprehensive review of all existing employee access accounts to ensure that network and system access granted is needed and compatible with user job responsibilities and adjusting user access accordingly.
- Reviewing file share rights to ensure unnecessary access is not granted to users.
- Removing or disabling employees' network and systems access immediately upon their termination.
- Reviewing all administrator access accounts to eliminate or minimize their use when possible.
- Requiring and enforcing password policies for all accounts (or users, as applicable) to change passwords on a periodic basis, including establishing requirements and time frames for changing service account passwords.

Agency Response: Concur

Agency: Department of Revenue
Name of contact person and title: Francis Becker, Senior Internal Auditor
Anticipated completion date: January 2017

The Department was previously written up for this same finding in a separate performance audit back in September of 2015. The timing of this finding dates back as far as 24 months, and since this time, the Department has made tremendous strides in remediating this finding. Specifically, the Department has fully implemented various information security program policies that address each point in this finding. The Department has been actively identifying, creating, and implementing associated procedures to accompany these policies. As these procedures are implemented, the Department conducts various analyses' to confirm that the Departments current practices mirror all applicable policies and procedures.

2015-09
The Department of Revenue should improve security over its information technology resources

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

Condition and context: The Department drafted new written policies to align with the State's guidance on best practices for state agencies to follow for IT security; however, these policies had not been fully implemented. As a result, the Department did not:

- Conduct a structured department-wide IT security risk assessment process that is performed at least annually and includes identification of threats and vulnerabilities, documentation of results, review by appropriate personnel, and prioritization of risk for remediation. In addition, the Department did not incorporate any risks identified as part of the IT security vulnerability scans performed into the IT security risk assessment process.
- Have a plan to remediate or mitigate identified threats and vulnerabilities.
- Have an adequate process to evaluate and test patches to ensure system functionality is not affected by recently released updates, verify the applicability of the patches applied to all IT resources, and ensure patches were up-to-date.
- Have a process in place to ensure its IT resources are configured securely.
- Identify and classify data by sensitivity and take appropriate action to protect sensitive information.
- Enter into written security agreements with local governments and businesses that access its IT resources that outline information system connections' security requirements.
- Proactively log and monitor key user and system security activity.
- Establish a process to respond to security incidents.
- Provide continuous training to keep IT personnel up to date on IT security risks, controls, and practices.

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

Cause: The Department's new policies have not been fully implemented.

Recommendation: To help ensure that the Department is able to effectively maintain and secure its IT resources, the Department should continue to implement its new policies over securing its IT resources and ensure that documented procedures are developed that include the following:

- Conducting an IT security risk assessment process at least annually that includes identification of risk scenarios that could impact the Department, including the scenarios' likelihood and magnitude; documentation and dissemination of results; evaluation by appropriate personnel; and prioritization of risks identified for remediation. Also, any threats and vulnerabilities identified as part of the Department's IT security vulnerability scans should be incorporated into the IT security risk assessment process.
- Developing a formal process for vulnerability scans that includes performing IT vulnerability scans on a periodic basis and utilizing tools and techniques to automate parts of the process by using standards for software flaws and improper configuration, formatting procedures to test for the presence of threats and vulnerabilities, and measuring the impact of identified threats and vulnerabilities. In addition, the Department should analyze vulnerability scan reports and results, remediate legitimate vulnerabilities as appropriate.
- Developing patch-management policies and procedures to ensure patches are evaluated, tested, and applied in a timely manner once the vendor makes them available.

- Configuring IT resources to provide only essential capabilities so that they do not provide more functionality than is necessary, including provisions and controls to ensure that unauthorized or unneeded software is not installed or used.
- Identifying, categorizing, and inventorying sensitive information and developing security measures to protect it, such as implementing controls to prevent unauthorized access to the information. The Department's policies and procedures should include the security categories into which information should be classified, as well as the state statutes and federal regulations that impact the categories.
- Establishing written security agreements with external organizations requiring access to its IT resources that outline IT resource connections' security requirements.
- Performing proactive logging and log monitoring. The Department should identify the IT resources and functions in each system that should be logged. Also, the Department should determine how frequently logs are monitored and who is responsible for ensuring that logging occurs and reviewing the logs. In addition, the Department should establish standard response actions for possible detected events, including reporting the security status of the Department and its IT resources to critical personnel. Finally, the Department should establish provisions for log security and retention.
- Establishing and documenting a process to identify and respond to security incidents. This process should include developing and testing an incident response plan and training staff responsible for the plan. The plan should define reportable incidents and address steps on how to identify and handle security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. The plan should also coordinate incident handling activities with contingency planning activities, and incorporate lessons learned from ongoing incident handling in the incident response procedures. The incident response plan should be distributed to appropriate personnel and updated, as necessary. Suspected incidents should be reported to individuals responsible for responding so incidents can be tracked and documented. The Department should also ensure these policies and procedures follow regulatory and statutory requirements, provide a mechanism for assisting users in handling and reporting security incidents, and make disclosures to affected individuals and appropriate authorities should an incident occur.
- Developing a plan to provide continuous training on IT security risks, controls, and practices for the Department's IT personnel. In addition, the Department should develop a training program for all employees that provides a basic understanding of information security, user actions to maintain security, and instructions on how to recognize and report potential indicators of security threats, including threats department employees generate. In addition, provide training for new users and on an on-going basis as determined by the Department.

Agency Response: Concur

Agency: Department of Revenue
Name of contact person and title: Francis Becker, Senior Internal Auditor
Anticipated completion date: January 2017

The Department was previously written up for this same finding back in September of 2015 in a separate performance audit report. The timing of this finding dates back as far as 24 months, and since this time, the Department has made tremendous strides in remediating this finding. Specifically, the Department has fully implemented various information security program policies that address each point in this finding. The Department has been actively identifying, creating, and implementing associated procedures to accompany these policies. As these procedures are implemented, the Department conducts various analyses' to confirm that the Departments current practices mirror all applicable policies and procedures. This includes enhancing the Departments new hire training, annual recertification training, and creating additional training mechanisms, such as computer based training, to keep Department employees abreast of its information security program policies and related requirements.

2015-10
The Department of Revenue should continue to strengthen its procedures for processing income tax revenues

Criteria: The Department of Revenue (Department) should continue to strengthen its procedures to ensure that it collects and reports all state income tax revenues.

Condition and context: The Department is responsible for collecting and reporting state income taxes. While testing procedures for income tax revenues, auditors noted additional procedures that the Department should perform to help ensure it achieves this. Because this finding is of a sensitive nature, its specific details, including detailed recommendations, were verbally communicated to those officials directly responsible for implementing the corrective action.

Effect: The State may not receive the proper amount of income taxes.

Cause: The Department's information system did not have the functionality to perform the identified omitted procedures.

Recommendation: The Department should implement additional procedures necessary to compensate for the omitted procedures.

This finding is similar to prior-year finding 2014-03.

Agency Response: Concur

Agency: Department of Revenue
Name of contact person and title: Francis Becker, Senior Internal Auditor
Anticipated completion date: Unknown

The Department will continue to expand its manual procedures over this process. To fully remediate this finding however, the Department must expand its current IT functionality over this process, which will require additional funding that is not currently available. The Department is continually implementing manual procedures to mitigate the associated risks and is currently researching automation tools that would efficiently and effectively remediate any remaining deficiencies over this process.

2015-11
The Department of Economic Security should update and test its disaster recovery plan over its information technology resources

Criteria: It is critical that the Department of Economic Security (DES) have a comprehensive, up-to-date disaster recovery plan for its information technology (IT) resources, which includes its systems, network, infrastructure and data, to provide for the continuity of operations and to ensure that it can recover information and data in the event of a disaster, system or equipment failure, or other interruption. Also, the plan should be evaluated, tested, and updated annually.

Condition and context: The DES had a disaster recovery plan for its IT resources; however, the Department did not evaluate, test, and update its plan annually. The Department of Child Safety (DCS) also uses these IT resources.

Effect: The DES and DCS risk disruption of operations; inaccurate or incomplete financial, federal program, or management information; expensive recovery efforts; and financial losses because of inadequate disaster recovery controls. In addition, service disruption in the event of a disaster, system or equipment failure, or other interruption could result in significant harm or inconvenience to the State and its citizens.

Cause: The DES did not follow its policies and procedures to ensure its disaster recovery plan was sufficiently tested and evaluated annually.

Recommendation: To help ensure the continuity of the DES and DCS operations and that electronic information and data are not lost in the event of a disaster, system or equipment failure, or other interruption, the DES should evaluate, test, and update its disaster recovery plan annually and retain documentation of all disaster recovery plan tests and those tests' results.

This finding is similar to prior-year finding 2014-05. This finding is also reported as a federal finding. See finding 2015-115.

Agency Response: Concur

Name of contact person and title: Lori J. Cunningham, Deputy Chief Information Officer
Anticipated completion date: June 30, 2018

The Division of Technology Services (DTS) agrees with the finding and provides the following action plan. Contingency Planning is comprised of both a Continuity of Operations Plan (COOP) focused on process continuity and a Disaster Recovery Plan focused on the supporting technology. This Corrective Action Plan addresses the disaster recovery findings of the OAG audit. The current Department of Economic Security (DES) Disaster Recovery Plan has been in place since 1999. There was a formal review of the Plan in 2006 and it was last updated in 2011. The last failover drill was completed in 2010 and included a failover to an IBM mainframe located in Boulder, Colorado. Currently encrypted data from the mainframe is simultaneously stored in a secondary secured location. For State Fiscal Year (SFY) 2015, DES received funding for moving the DES Data Center into a purpose built, Tier III data center operated by a third party. The facility risk of outages is anticipated to be greatly reduced by this move. DES is on schedule to complete this move by end of SFY16.

Over the last 6 months, DTS has made significant strides in ensuring the reliability and availability of customers' data. Notably due to two significant accomplishments:

- With the acquisition of new technology that addresses data stored on tape, DTS can now say that 100% of all Mainframe Data (both disk and tape {virtual}) is dynamically duplicated and encrypted at a remote secure site. Because of this, there can be no loss of mainframe data due to an incident (disaster) that occurs at the primary or backup Datacenter.
- Along with the launching of this new data storage technology, DTS has executed three disaster recovery drills during 2015 that take advantage of this new infrastructure. These drills were iterative in nature and designed to validate the availability of timely backup data, along with the ability to process and present this data in a manner that is identical to our current production environment. Validation and testing continues on a regular basis. The Disaster Recovery architecture being utilized during our drills eliminates the need to 'restore' data, traditionally a lengthy process requiring off-site tape being transported and loading of databases onto disk drives for access. Our mirrored data environment guarantees that user and program data is stored simultaneously and identically at two separate physical locations, thus eliminating the need to restore.

Milestones and Anticipated Completion Dates

A. Migrate the data center to new location --COMPLETED
B. Review and modify Recovery Plan -- SFY17
C. Perform annual test -- SFY16 testing completed prior to data center relocation. The DTS continues working toward full annual DR testing as problems are discovered and resolved
D. Document overall testing strategies, testing frequencies, and test results—SFY17 on target
E. Implement technology appropriate to ensure continuity of operations—SFY18 will see DES creating a disaster recovery environment with implementation and testing of this new environment in SFY18

Other auditors' findings:

The other auditors who audited the Arizona Department of Transportation, the Arizona Health Care Cost Containment System, and the Arizona State Lottery reported the following corrective action plans:

2015-12
Sub-ledger Reconciliations

Criteria: Internal controls would dictate that procedures be designed, implemented and followed for the reconciliation of general subledger accounts to prevent, detect and correct potential misstatements.

Condition: Due to a change in administration, key personnel, as well as an implementation of a significant entity wide system upgrade, the Arizona Department of Transportation did not have a system of internal controls that would enable management to timely and properly reconcile the general ledger subledger accounts to ensure they were complete and presented in accordance with accounting principles generally accepted in the United States in a timely manner.

Effect: There were misstatements of various general ledger accounts that resulted in material audit adjustments.

Cause: Reconciliation procedures were not performed timely and controls were either not properly designed or implemented, or designed controls were not performed as designed.

Recommendation: In order to strengthen internal controls, we recommend management review its current policies and determine whether the policies should be revised. We also recommend management review the implementation of current procedures to determine that procedures are being performed as designed.

Agency Response: Concur

Name of contact person and title: Tim Newton, Controller

The Arizona Department of Transportation (ADOT) concurs with the finding and is actively working on implementing controls that will help prevent, detect and correct material misstatements. The implementation of the new statewide financial system (AFIS) greatly impacted the Arizona Department of Transportation's ability to prepare the Comprehensive Annual Financial Report. Specifically, the reporting functionality within the new system was not fully developed which made it very difficult to calculate accrual data. The Arizona Department of Transportation is in the process of developing our own data warehouse which will improve reporting capabilities and is also contracting with a consulting firm to develop and implement appropriate controls. It is anticipated that preliminary controls will be in place by June 30, 2016 with more mature controls being developed over the following 12 months.

2015-13
Year-End Adjustments and Preparation of the Financial Statements

Criteria: Internal controls would dictate that an adequate review process be put in place to prevent a material misstatement from going undetected and uncorrected.

Condition: Due to a change in administration, key personnel, as well as an implementation of a significant entity wide system upgrade, the Arizona Department of Transportation did not have a system of internal controls that would enable management to conclude the financial statements and related disclosures, and the schedule of expenditures of federal awards were complete and presented in accordance with accounting principles generally accepted in the United States of America in a timely manner.

The Arizona Department of Transportation requested us to assist in drafting the financial statements. We also proposed material audit adjustments in order to draft the financial statements. These entries related to internal controls over the year-end close-out process. The absence of a complete control procedures or processes in this area is considered a material weakness because there were material misstatements of the financial statements that occurred and not prevented or detected by Arizona Department of Transportation's internal control processes.

Effect: Audit adjustments were proposed and subsequently approved and recorded by management to present the financial statements in accordance with generally accepted accounting principles. Those entries included:

1) Audit adjustments were proposed and subsequently recorded by management to properly record beginning fund balances.
2) Audit adjustments were proposed and subsequently recorded by management to properly report cash balances and outstanding warrants (checks).
3) Audit adjustments were proposed and subsequently recorded by management to properly report accounts payable, capital outlay and expenditures.
4) Audit adjustments were proposed and subsequently recorded by management to properly report accounts receivable, deferred inflows of resources and revenue.
5) Audit adjustments were proposed and subsequently recorded by management to properly record distributions to Arizona counties and cities that were improperly capitalized during the year.
6) Audit adjustments were proposed and subsequently recorded by management to properly report interfund balances and transfers.

Cause: The finance department did not have an adequate conversion processes and personnel to prepare the year-end financial statements for external reporting purposes.

Recommendation: We recommend the Arizona Department of Transportation continue to evaluate its internal control processes to determine if additional internal control procedures should be implemented to identify year end closing adjustments. Should the Arizona Department of Transportation elect to establish the "full oversight" of the financial statement preparation, we suggest management establish effective review policies and procedures, including, but not limited to, the following functions: review the adequacy of financial statement disclosures by completing a disclosure checklist; review and approve schedules and calculations supporting the amounts included in the notes to the financial statements; apply analytic procedures to the draft financial statements; and perform other procedures considered necessary by management.

Agency Response: Concur

Name of contact person and title: Tim Newton, Controller

The Arizona Department of Transportation concurs with the finding and is actively working on implementing controls that will help prevent, detect and correct material misstatements. The implementation of the new statewide financial system (AFIS) greatly impacted the Arizona Department of Transportation's ability to prepare the Comprehensive Annual Financial Report. Specifically, the reporting functionality within the new system was not fully developed which made it very difficult to calculate accrual data. The Arizona Department of Transportation is in the process of developing our own data warehouse which will improve reporting capabilities and is also contracting with a consulting firm to help develop and implement appropriate controls. It is anticipated that preliminary controls will be in place by June 30, 2016 with more mature controls being developed over the following 12 months.

2015-14
Improve controls over purchasing and disbursements

Criteria: A strong and efficient system of internal controls over purchasing and disbursements is critically important to governmental organizations. Internal Controls over the purchasing, procurement, contracting and accounts payable processes should be established and maintained to include limitations on purchasing authority, proper segregation of duties, and appropriate reviews of invoices and warrants.

Condition: During fiscal year 2015, an Arizona Health Care Cost Containment System (AHCCCS) internal investigation identified an employee embezzlement. The embezzlement involved AHCCCS' Contracts and Purchasing Administrator, who used their position to initiate and approve vendor invoices related to a multi-service contract. The Contracts and Purchasing Administrator was then able to use his long tenure and standing within AHCCCS to obtain possession of the paper warrants prior to their mailing to the vendor. In many instances, the vendor invoices were fraudulent. However, in some instances, the vendor invoices were legitimate and the invoices were subsequently adjusted off by the vendor for an unknown reason. AHCCCS believes the fraud occurred over a ten-year period (2006-2015) and the total cumulative amount misappropriated is estimated at $5,757,728. The funds were misappropriated from AHCCCS' administrative budget, which approximates $200 million annually.

Effect: For the period from fiscal year 2006 through fiscal year 2015, AHCCCS estimates that their Contracts and Purchasing Administrator misappropriated $5,757,728 of fraudulent vendor payments under a multi-service contract. The funds were misappropriated from AHCCCS' administrative budget, which approximates $200 million annually. See findings 2015-127 for effect on federal awards administered by AHCCCS.

Cause: Using his authority, tenure and standing within AHCCCS, the Contracts and Purchasing Administrator was able to circumvent existing controls to misappropriate funds. The Contracts and Purchasing Administrator had the authority to initiate and approve the vendor invoices under his delegated procurement authority and position. Additionally, he was able to use his long tenure and standing within AHCCCS to obtain possession of the paper warrants prior to their mailing to the vendor.

Recommendation: We recommend that AHCCCS review their existing internal control environment surrounding purchasing and disbursements to limit delegated procurement authority and to ensure proper segregation of duties. We also recommend that AHCCCS enforce its existing policies to ensure that the distribution of paper warrants, as well as the review and approval of any paper warrants prior to their distribution, must be segregated from individuals who initiate a purchase requisition and or the payment request. Finally, we recommend that AHCCCS periodically audit vendor accounts and reconcile vendor receipt detail to AHCCCS payment detail.

This finding is also reported as a federal finding. See finding 2015-127.

Agency Response: Concur

Name of contact person and title: Jeffery Tegen, Assistant Director
Anticipated completion date: December 31, 2015

Arizona Health Care Cost Containment System (AHCCCS) will ensure assets are properly safeguarded and controlled and internal control policies and procedures are reviewed, strengthened and followed so that no single individual has control over the purchasing process to initiate a transaction, approve that transaction and have access to the paper warrant. AHCCCS has contracted with an Independent CPA to review, assess and provide recommendations for purchasing and accounts payable internal control policies and procedures. The Agency has worked with the Arizona State Procurement Office to reduce the previously unlimited delegation authority to a revised limited delegated procurement authority of $10,000. In addition, AHCCCS has established a policy that all payment transactions must utilize the central warrant mailing service provided by the Arizona Department of Administration – General Accounting Office in conjunction with the July 1, 2015 implementation of the new Statewide Accounting System. Finally, AHCCCS will aggressively prosecute the accused former employee and exhaust all available remedies to recover all embezzled assets in the timeliest manner possible.

2015-15
Accounting and reporting components of net position

Criteria: For the Arizona State Lottery (Lottery), we believe that paragraph 12.117 of the American Institute of Certified Public Accountants, (AICPA) State and Local Governments Audit and Accounting Guide provides the relevant accounting guidance for liabilities for prizes and forfeitures of unclaimed prizes. Forfeitures of unclaimed prizes should be recognized as a gain (net against prize expense) as of the date the claim is forfeited according to the provisions of a State's stated regulations. Many States have regulations with regard to how forfeited unclaimed prizes must be utilized. For example, some States require all forfeited unclaimed prizes be transferred to another State fund or agency having a different mission. Arizona Revised Statutes 5-568 states the following:

Disposition of unclaimed prize money
Unclaimed prize money for the prize on a winning ticket or share shall be retained for the person entitled to the prize for one hundred eighty days after the drawing in which the prize was won in the case of a drawing prize and for one hundred eighty days after the announced end of the game in question in the case of a prize determined in any manner other than by means of a drawing. If a claim is not made for the money within the applicable period, seventy per cent of the prize money shall be held in the state lottery prize fund for use as additional prizes in future games and thirty per cent shall be transferred monthly to the court appointed special advocate fund established by section 8-524.

We believe the State's statute places a restriction on the use of forfeited prizes. Restricted net position should be reported when constraints placed on net position are either externally imposed by grantors, creditors, contributors, or by laws or enabling legislation. The restriction to use unclaimed prizes that are forfeited represents a specific purpose, does not represent a liability in our view, rather it is the underlying transaction exchange transaction resulting from the sale of lottery tickets for games in progress that creates a liability, defined by GASB's Concept Statement No. 4, *Elements of Financial Statements*, as the present obligation to sacrifice resources.

Condition: The previous balance reported as liabilities for prizes was comprised of several components of the Lottery's Prize Fund. These components consisted of unclaimed forfeited prizes, accumulated prize fund balance, accumulated investment earnings of the prize fund, and flows of the prize fund. Certain of these components do not appear related to a present obligation for prizes. The Arizona Lottery retains and reports unclaimed prizes as a liability.

Context: Management's estimate of liability attributable to only prizes is approximately $20.8 million. A portion of this estimate is attributable to forfeited prizes is approximately $5.7 million.

Effect: We believe the liability for prizes has been overstated and that components of net position are understated or other liabilities exist.

Cause: We do not believe management had fully considered the applicable accounting and financial reporting guidance for prizes or components of net position.

Recommendation: We recommend that management review the underlying nature and agreements for each significant reported balance and assess reporting restricted components of net position and review/revise its accounting policies with regard to activities of the *Prize Fund*. Those policies should reflect the use of resources in conformity with State statute while also considering the financial condition of the Lottery.

This finding is similar to prior-year finding 2014-07.

Agency Response: Concur

Agency: Arizona State Lottery

Management will review accounting policies for activities in the Prize Fund. The Lottery has been consistent in its reporting of prize liability since the Lottery's inception and that reporting is similar to reporting used by other state lotteries. We agreed with the auditor to revise the presentation of prize liability this year and will seek to find an appropriate presentation in future years.

2015-16
Regularly review third-party service reports

Criteria: Third party service organizations are entities that provide outsourcing activities that are relevant to the control environments at user organizations. The Statements on Standards for Attestation Engagements (SSAE) No. 16, Type II, report is an independent auditor's report on the design and operating effectiveness of key controls at a service organization. A SSAE No. 16 Type II, report provides assurance to user organizations that the control objectives relating to the services provided by their service organization are suitably designed and operating effectively throughout the examination period.

Condition and context: The Arizona State Lottery (Lottery) utilizes reports and systems of GTECH, a service organization; however, GTECH does not currently provide a SSAE No. 16, Type II, report to the Lottery.

Effect: Errors, if any, in the reports provided to the Lottery by GTECH may not be detected in a timely manner.

Cause: GTECH does not appear to have a Type II SSAE 16 report available for the Lottery.

Recommendation: We recommended that management obtain and review SSAE No. 16/SAS 70 report annually to ensure service providers have sufficient controls in place and are operating effectively given the significance of the information provided by GTECH to the Lottery.

This finding is similar to prior-year finding 2014-08.

Agency Response: Concur

Agency: Arizona State Lottery

We have formally requested IGT (formerly GTech) to complete a SOC Report, type II for period of nine months 07/01/15 through 03/31/16 to remedy this finding.