

DOUGLAS A. DUCEY  
Governor



MARK W. KILLIAN  
Director

# Arizona Department of Agriculture

1688 W. Adams Street, Phoenix, Arizona 85007  
(602) 542-0990 FAX (602) 542-5420

September 24, 2020

Lindsey Perry  
Auditor General  
2910 North 44<sup>th</sup> Street, Suite 410  
Phoenix, AZ 85018

Dear Ms. Perry:

I have reviewed the revised preliminary report draft of the performance audit and sunset review of the Arizona Department of Agriculture. Enclosed is the Department's written response to the report.

Respectfully,

Mark W. Killian  
Director

## **Finding 1:** Department did not comply with some conflict-of-interest requirements

**Recommendation 1:** The Department should comply with statutory conflict-of-interest requirements and best practices, including:

**Recommendation 1a:** Ensuring all employees and public officers complete an annual conflict-of-interest disclosure form.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Department will send an email annually to all employees and members of the various councils with the conflict-of-interest statutes attached and a copy of the conflict-of-interest disclosure form and ask them to declare any new possible conflicts from the prior year. The conflict-of-interest disclosure form will be sent out on a calendar year.

**Recommendation 1b:** Using a conflict-of-interest disclosure form that addresses both financial and decision-making conflicts-of-interest.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Department has adopted the new ADOA form for the annual disclosure form. New hires complete the form online.

**Recommendation 1c:** Storing all substantial interest disclosures in a special file.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Department already has established a separate file for disclosure statements.

**Recommendation 1d:** Establishing a process to review and remediate disclosed conflicts.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: Human Resources will work with senior staff to establish a process to review disclosure forms.

**Recommendation 2:** The Department should update and implement its policies and procedures to comply with all the State's conflict-of-interest requirements and best practices.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: Human Resources will review established policies and update where needed to comply with State requirements.

**Recommendation 3:** The Department should develop and implement periodic training on its conflict-of-interest requirements, process, and form, including providing training to all employees and public officers on how the State's conflict-of-interest requirements relate to their unique program, function, or responsibilities.

Department Response: The finding of the Auditor General is agreed to and a different method of dealing with the finding will be implemented.

Response explanation: Since the Department has only one Human Resources person, the Department will determine the best course of action to ensure that all individuals are aware of the issues within their program that may be considered a conflict-of-interest according to State statute.

**Finding 2:** Department did not effectively safeguard its IT systems and sensitive data

**Recommendation 4:** The Department should conduct an annual risk assessment of its IT systems to evaluate, document, and prioritize the areas in its IT systems with the highest security risks, as required by ASET. As part of this effort, the Department should use the information obtained from risk assessments to address identified risks.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Department will work with ADOA-ASET to determine the best practices for annual IT security risk assessment. While the Department has not been following a formal process, it has been making a major effort to improve security and reduce risk to its IT infrastructure with guidance from ADOA-ASET.

**Recommendation 5:** The Department should incorporate security requirements prescribed by ASET and recommended by credible industry standards into its web application development to address potential vulnerabilities and help ensure its web applications are secure.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Department agrees to incorporate security requirements as best it can. The Department does not have the resources in manpower, budget, and often time, to perform the due diligence it would prefer to undertake. Third-party experts have performed penetration testing on these applications and they had not found credible evidence to suggest the Department's applications are vulnerable to external attack. An independent study by the Nerdy, commissioned by ADOA, found that the Department is understaffed, but its processes were sound given the circumstances. It recommended a budget of just under \$16 million spent over five years to completely modernize the Department. Without additional resources, IT is forced to deal with issues as they arise just to keep the systems operational. The Department often doesn't get to pick and choose which projects to focus on. However, IT does operate using modern tools and platforms starting with a secure, proven infrastructure. At this point in time, most new applications involve porting code from older platforms onto the new platforms without fundamentally changing how they were constructed. Security and reliability is improved feature by

feature as needed by the customers. Once the migration to a modern platform has been completed, the Department will be able to take a more standard approach to unifying, securing and implementing new development.

**Recommendation 6:** The Department should appropriately manage web application accounts in accordance with ASET policies and recommended credible industry practices.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: As part of the Department's migration to new servers, it is given the opportunity to revise and simplify the security structure used by its applications. The Department will implement a quarterly audit of user accounts.

**Recommendation 7:** The Department should continue to ensure that vulnerability scans of its IT systems are performed.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: Scans, which are performed by ADOA-ASET, are supposed to occur every two weeks. The Department reviews the results monthly.

**Recommendation 8:** The Department should ensure that contractors using its IT systems complete annual IT security awareness training.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: Contractors will take IT security awareness training upon the start of their contract and annually thereafter.

**Recommendation 9:** The Department should develop and implement an IT security governance framework, as required by ASET policy and recommended by credible industry standards, that includes the following:

**Recommendation 9a:** Reviewing, modifying as needed, and implementing its draft IT security policies and procedures. As part of this process, the Department should ensure that its policies and procedures:

- Describe how those charged with IT security governance will safeguard IT systems and data, such as ensuring annual risk assessments are performed.
- Define staff roles and responsibilities.
- Address ASET requirements and credible industry standards for web application development, such as gathering security requirements, using secure coding standards, performing threat modeling, and reviewing source code.
- Require that user account access and account privileges be reviewed periodically.
- Require that accounts for terminated employees be disabled or removed as soon after the employee leaves as is practical.

- Require that all sensitive data be accessible only to those who need it to perform their job duties.
- Require that all staff and contractors who have access to or use its IT systems complete annual security awareness training and establish processes for tracking compliance with this requirement.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Department will continue to review and implement Department and State policies to bring the Department up-to-date with guidance from ADOA-ASET.

**Recommendation 9b:** Working with ASET to define and document the scope of IT security services that ASET provides and ensure that ASET provides these services.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Department will work with its Engagement Manager to ensure it knows of and understands the ADOA-ASET services they provide in the form of a Service Agreement.

**Recommendation 9c:** Incorporating IT security performance measures into its strategic plan and using the measures to monitor progress toward achieving its IT security-related goals and objectives.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Department will expand its current IT security performance measures to fully implement this recommendation.

**Sunset Factor 2:** The extent to which the Department has met its statutory objective and purpose and the efficiency with which it has operated.

**Recommendation 10:** The Department should conduct an annual physical inventory of its capital assets and maintain clear, accurate, and complete information for its capital assets in the State's accounting system so that the capital assets can be easily identified during annual physical inventory.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Department is in the process of updating its fixed and memo asset records in AFIS in order to have complete information needed to conduct a valid physical inventory.

**Recommendation 11:** The Department should remove assets that have been disposed or transferred from the State's accounting system within the SAAM required time frame.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Department is in the process of removing assets that previously have been disposed of and will keep current with removals going forward.

**Recommendation 12:** The Department should develop policies and procedures for all areas required by the SAAM, including policies and procedures for handling cash payments, administering and using p-cards, and requesting reimbursement for travel expenses, including lodging and meals.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Department always has strived to stay within policies set forth in SAAM and did not realize that internal policies also were a necessity. Internal policies will be created on the aforementioned subjects.

**Recommendation 13:** The Department should continue to work with ADOT to ensure that the Department's take-home vehicle policies and procedures incorporate the requirements from the finalized State-wide guidelines.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Department will follow ADOT guidelines.

**Sunset Factor 5:** The extent to which the Department has encouraged input from the public before adopting its rules and the extent to which it has informed the public as to its actions and their expected impact on the public.

**Recommendation 14:** The Department should ensure that it posts meeting notices and agendas on its website and at the Department at least 24 hours before public meetings for all the councils and committees it supports and make council and committee meeting minutes or a recording of these public meetings available for public inspection within 3 working days following a meeting.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Department will remind all employees that staff the councils and committees of all of the above public meeting requirements.

**Recommendation 15:** The Department should include a disclosure statement on its website stating where all public meeting notices for all councils and committees will be posted.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Department will post on its website disclosure statements for the Citrus, Fruit and Vegetable Advisory Council, Animal Services Division Council, Arizona Leafy Greens Food Safety Committee, Industrial Hemp Advisory Council, Pesticide Advisory Committee, Pest Management Division Council, and Weights and Measures Services Division Council.

**Sunset Factor 6:** The extent to which the Department has been able to investigate and resolve complaints that are within its jurisdiction.

**Recommendation 16:** The Department should ensure that all complaints are investigated and resolved in a timely manner.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: With one exception, the Department will work to ensure that all complaints are investigated and resolved in a timely manner. The Sunset Review report stated that the Department did not investigate the complaints it received related to medical marijuana because it believed that it lacked the authority to enter medical marijuana facilities. The Department will work with licensed scale owners and other stakeholders to identify a way for these scales to be inspected.

**Recommendation 17:** The Department should notify complainants about the status of complaint investigations, as required by Department policy.

Department Response: The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Response explanation: The Department will notify complainants about the status of complaint investigation.