

The September 2020 Arizona Department of Agriculture performance audit and sunset review found that the Department did not comply with all statutory conflict-of-interest requirements and effectively safeguard its IT systems and sensitive data. We made 22 recommendations to the Department, and its status in implementing the recommendations is as follows:

Status of 22 recommendations

Implemented	11
In process	11

We will conduct a 36-month followup with the Department on the status of the recommendations that have not yet been implemented.

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

1. The Department should comply with statutory conflict-of-interest requirements and best practices, including:
 - a. Ensuring all employees and public officers complete an annual conflict-of-interest disclosure form.
Implemented at 24 months
 - b. Using a conflict-of-interest disclosure form that addresses both financial and decision-making conflicts of interest.
Implemented at 6 months
 - c. Storing all substantial interest disclosures in a special file.
Implemented at 24 months
 - d. Establishing a process to review and remediate disclosed conflicts.
Implementation in process—The Department has developed a conflict-of-interest policy that includes a supervisory review process for reviewing conflict-of-interest disclosure forms. However, the policy does not include a process for remediating disclosed conflicts.
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.
Implementation in process—The Department has developed a conflict-of-interest policy that addresses various statutory and best practice requirements, including requiring employees to submit an annual conflict-of-interest disclosure form, reviewing conflict-of-interest disclosure forms, and prohibiting employees from participating in decisions for which they have a substantial interest. However, the policy does not address remediating disclosed conflicts (see explanation for Recommendation 1d).
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.

Implementation in process—The Department has developed a training presentation on its conflict-of-interest requirements, process, and form, and reported that it will provide this training to all new employees during the onboarding process. Additionally, the Department reported that each of its divisions will be required to conduct this training for its current staff in January 2022. We will further assess the Department’s implementation of this recommendation during our 36-month followup.

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

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.

Implemented at 24 months

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.

Implementation in process—The Department has implemented some security requirements prescribed by ASET and recommended by credible industry standards to ensure its web applications are secure, such as conducting weekly code reviews and requiring role-based security training. However, the Department reported that it would not be able to implement all security requirements for web application development until June 2023 because of limited staffing resources and prioritizing other time sensitive IT projects. We will further assess the Department’s implementation of this recommendation during our 36-month followup.

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

Implementation in process—Since our initial followup, the Department has taken additional steps to appropriately manage its web application accounts, such as developing account management and access control policies. The Department reported it plans to implement remaining policies for appropriately managing web accounts by January 2023, including policies for onboarding and offboarding staff who use web applications and deleting inactive employee accounts to help ensure only active employees have access to its web applications. We will further assess the Department’s implementation of this recommendation during our 36-month followup.

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

Implemented at 6 months

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

Implemented at 24 months

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:

- a. 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.

Implementation in process—The Department revised its IT policies and procedures to include all information required by ASET policy and recommended by credible industry standards, including describing staff roles and responsibilities and restricting access to sensitive data. We will review the Department's implementation of these policies and procedures during our 36-month followup.

- b. Working with ASET to define and document the scope of IT security services that ASET provides and ensure that ASET provides these services.

Implemented at 24 months

- c. 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.

Implementation in process—The Department developed an IT strategic plan for fiscal year 2024 that includes IT security-related goals and objectives, and developed associated performance measures, which it has also incorporated into its IT strategic plan. We will further assess the Department's use of the performance measures to monitor its progress toward achieving its security-related goals and objectives during our 36-month followup.

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

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.

Implementation in process—The Department created a list of agency assets in December 2021 and is working to verify the location of its assets. The Department reported that it is still working on locating some items or conducting research to determine if they were disposed of and need to be removed. It did not provide a date for when its research would be completed. We will further assess the Department's implementation of this recommendation during our 36-month followup.

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

Implementation in process—Although the Department has removed some disposed assets from the State's accounting system, it has yet to identify all assets that it has disposed of and needs to remove from the system (see explanation for Recommendation 10). We will further assess the Department's efforts to remove assets from the State's accounting system within the required time frame during our 36-month followup.

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.

Implementation in process—The Department has begun drafting policies and procedures for administering and using p-cards and reported that it is working on developing policies and procedures for all areas required by the SAAM. The Department reported that it plans to finalize these policies and procedures by the end of March 2023. We will further assess the Department's implementation of this recommendation during our 36-month followup.

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.

Implemented at 24 months

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.

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.

Implemented at 6 months

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.

Implemented at 6 months

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

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

Implemented at 6 months

17. Notify complainants about the status of complaint investigations, as required by Department policy.

Implementation in process—Although the Department notified complainants monthly about the investigation status for 2 of 4 complaints we reviewed, it did not consistently notify complainants monthly for the other 2 complaints. We will continue to assess the Department's compliance with its policy to notify complainants monthly during our 36-month followup.