ARIZONA Auditor General
Making a Positive Difference

Arizona Department of Health Services

72-Month Followup of Conflict-of-Interest, IT Security, and Other Recommendations from Sunset Review Report 19-112

The September 2019 Arizona Department of Health Services performance audit and sunset review found that the Department did not comply with some conflict-of-interest requirements and had some gaps in 4 IT security areas.[1] We made **12** recommendations to the Department related conflict-of-interest, IT security, and other issues identified in the sunset factors section of the 2019 report.[2]

Department's status in implementing 12 recommendations

Implementation status	Number of recommendations
Implemented	2 recommendations
Partially implemented	3 recommendations
In process	7 recommendations

The Joint Legislative Audit Committee (JLAC) has directed our Office to conduct the Department's next sunset review, which is due October 1, 2027. As a result, rather than conducting a separate followup of the outstanding recommendations, we will conduct work to follow up on the Department's efforts to implement the 7 outstanding recommendations discussed in this followup during its sunset review, which we initiated in August 2025. Therefore, unless otherwise directed by JLAC, we have concluded our separate followup work on these 7 outstanding recommendations from the September 2019 report.

---

1 The first performance audit focused on the Department's administration of the Medical Marijuana Program. The second report addressed the Department's processes for procuring goods and services through contracts, monitoring contracts and agreements to ensure requirements are met, and processing payments for contracts and agreements. The third report addressed the Department's administration of the Arizona State Hospital. For more information on the other performance audits we issued as part of the Department's sunset review, including any applicable followup reports, see Report 19-107, 19-109, and 19-111.

2 See our 48-Month followup report on Long-Term Care Complaints and Self-Reports for the implementation status of the 5 recommendations from Finding 1 in our September 2019 Arizona Department of Health Services performance audit and sunset review and 4 additional recommendations we made during our 30-month followup.

Recommendations to the Department

Finding 2: Department did not comply with some conflict-of-interest requirements

3. The Department should continue its efforts to develop and implement a new conflict-of-interest disclosure process and form that will help it comply with the State's conflict-of-interest requirements and best practices, such as having public officials and employees annually disclose whether or not they have any substantial financial and/or decision-making conflicts, and train employees on how the State's conflict-of-interest requirements relate to their unique program, function, or responsibilities .

- Status: **Implemented at 18 months**

Finding 3: Some gaps in Department IT security processes resulted in a security incident and additional IT security weaknesses

4. The Department should develop and implement web application development policies and procedures that incorporate security into the development and modification process, including requirements for gathering security requirements, using up-to-date secure coding standards, performing threat modeling during development, reviewing source code, and performing security testing before releasing a web application to the live environment.

- Status: **Implementation in process**

  The Department continues to take steps toward implementing recommendations to safeguard its IT systems and data from misuse, attack, or loss. For example, the Department updated various policies and procedures, including its web application development policies and procedures to include required components, such as gathering security requirements and performing security testing, and is in the process of incorporating these policies into its processes.[3] Additionally, the Department revised its data-classification policies and procedures to provide guidance on how to classify its data and has developed a data-classification inventory. According to the Department, it also only allows contractors and staff to use State-provided devices to access work-related data. Further, the Department updated its risk-assessment policy and procedures to include a risk-report template used as part of its annual risk-assessment review for categorizing the Department's information based on the likelihood of risk and magnitude of harm. Although the Department provided documentation regarding its fiscal year 2026 annual risk assessment that documents information such as a description of risks identified, the risk owner, and risk scores, it did not provide additional information such as its prioritization and action plan to address the identified risks.

[3] The Department also provided a spreadsheet showing it is in the processs of testing various applications.

Finally, the Department has developed draft security-awareness training and education policies and procedures that cover areas such as requiring employees and contractors to comply with annual basic security-awareness and federal Health Insurance Portability and Accountability Act (HIPAA) training requirements and acceptable-use attestations, and how it will communicate security-awareness training throughout the year. The draft policies and procedures also contain role-based training matrices for specific roles, such as contracting officers and risk managers. We will further assess the Department's implementation of its policies, procedures, and trainings regarding its responsibility to safeguard its IT systems and data from misuse, attack, or loss during its sunset review, which we initiated in August 2025.

5. The Department should require staff who are responsible for developing web applications to regularly receive role-based training on how to develop and maintain secure web applications.

- Status: **Implementation in process**

  See explanation for Recommendation 4.

6. The Department should develop and implement revised data classification policies and procedures that provide guidance on how to classify its data; require developing a data classification inventory that is updated regularly; specify requirements for protecting data based on its level of risk; and establish processes for handling confidential data, such as ensuring that only approved devices process confidential data.

- Status: **Implementation in process**

  See explanation for Recommendation 4.

7. The Department should conduct a formal Department-wide risk assessment at least annually, as required in its risk assessment policy and procedures, to evaluate, document, and prioritize the areas in the Department's IT environment with the highest security risks.

- Status: **Implementation in process**

  See explanation for Recommendation 4.

8. The Department should develop and implement a revision to its risk assessment policy and procedures to include categorizing the Department's information based on the likelihood of risk and magnitude of harm as required by ASET policy.

- Status: **Implementation in process**

  See explanation for Recommendation 4.

9. The Department should develop and implement revised security awareness training policies and procedures that include a process for ensuring employees and contractors comply with annual basic security awareness and HIPAA training requirements and acceptable use attestations; specify the role-based training that is required based on employees' and

contractors' responsibilities; explain how it will implement its security awareness program; describe the topic areas that its security awareness training classes should cover; and specify how it will communicate security awareness training throughout the year.

- Status: **Implementation in process**

  See explanation for Recommendation 4.

10. The Department should continue with its plans to develop and implement role-based training.

- Status: **Implementation in process**

  See explanation for Recommendation 4.

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

11. The Department should continue using the electronic grants management system, and ensure that for all future grant evaluations conducted using this system its grant evaluations clearly indicate whether grant applicants complied with all evaluation criteria and that all evaluation factors are included in the grant solicitation.

- Status: **Implemented at 72 months**

  The Department continues to use its electronic grants-management system for grant evaluations to indicate whether grant applicants complied with all evaluation criteria and that all evaluation factors are included in the grant solicitation. Specifically, our review of a judgmental sample of 3 of 9 grants the Department awarded in calendar year 2024 found that the grant evaluations indicated if grant applicants complied with evaluation criteria and that evaluation factors were included in the grant-solicitation instructions.

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.

12. The Department should develop and implement policies, procedures, and training to help guide the boards, commissions, and councils it supports; and its staff members' compliance with open meeting law requirements.

- Status: **Partially Implemented at 72 months**

  As reported during our 30-month followup, the Department created an open meeting law policy and procedures in June 2022. This policy requires members of Department public bodies and Department staff responsible for providing support and oversight to these public bodies to annually take the Arizona Ombudsman Citizens' Aide Open Meeting Law training. However, although the policy requires Department staff and associated divisions within the Department to monitor that members of public bodies

complete the training, the Department lacks a centralized tracking process, and as of September 2024, only 41 of the more than 200 board, commission, and council members and support staff have completed the training.[4] The Department reported that it is in the process of training the individuals who have not completed the mandatory training.

Further, our review of 5 meetings subject to open meeting laws between July 2023 and October 2024 found that 4 of the public bodies complied with open meeting laws, such as timely posting their public meeting notices and making meeting minutes available. However, although 1 public body complied with most open meeting laws, it did not completely document the voting stance of all it members.

Finally, as part of the Department's sunset review, which we initiated in August 2025, we will evaluate the Department's continued efforts to develop and implement policies, procedures, and training to help guide the boards, commissions, and councils it supports; and its staff members' compliance with open meeting law requirements.

13. The Department should develop and implement an oversight process to ensure that the boards, commissions, and councils it supports comply with open meeting law requirements.

- Status: **Partially Implemented at 72 months**

  See explanation for Recommendation 12.

14. The Department should update its website to include a conspicuously posted statement indicating the location for all electronic and physical postings of public meeting notices and a complete and accurate listing of all the entities that are subject to open meeting law along with information about their purposes and where to locate information about these entities' public meetings, such as agendas and minutes.

- Status: **Partially Implemented at 30 months**

  As reported in our 6-month followup, the Department had updated its website to include a statement indicating the location for all electronic and physical postings of public meeting notices. During our 30-month followup, the Department reported that the list of open meeting law entities found on its website was complete and accurate. However, we identified 1 entity subject to open meeting law requirements that was not listed on the Department's website.

[4] Based our review of the Department's public meeting website and meeting minutes, we identified more than 200 board, commission, and council members and support staff. The Department has not developed a comprehensive list of all members and support staff for the boards, commissions, and councils it supports.