ARIZONA
AuditorGeneral
Making a Positive Difference

Arizona Department of Health Services Performance Audit and Sunset Review—Conflict-of-Interest, IT Security, and Other Recommendations
30-Month Follow-Up Report

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. We made 12 recommendations to the Department and its status in implementing the recommendations is as follows:[1]

Status of 12 recommendations

Implemented:	1
Partially implemented:	1
In process:	10

We will conduct a 42-month followup with the Department on the status of the recommendations that have not yet been implemented.

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.

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.

Implementation in process—The Department has finalized its draft Secure Coding Standards and developed new draft Secure Code Review Guidelines that include guidance for using up-to-date secure coding standards, performing threat modeling, and reviewing source code before releasing a web application. However, the Department's standards do not provide sufficient guidance for gathering security requirements or performing security testing. For example, as determined during the previous followup, although the Department's standards include some guidance on gathering some security requirements, they do not provide guidance on how to ensure each newly developed or modified web application is appropriately classified based on the data within that web application. Additionally, the Department has started performing some security testing and reported that it is in the process of implementing its plans to have its developers gain the skills and expertise needed to perform security testing on all Department web applications (see explanation for Recommendation 10 for more information on role-based training). The Department reported that it plans to implement its Secure Coding Standards and Secure

[1] See our 30-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.

Code Review Guidelines by the end of December 2022. We will continue to assess the Department's efforts to implement the IT security-related recommendations (Recommendations 4 through 10) during our 42-month followup.

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.

   Implementation in process—Although the Department has finalized the selection, content, and frequency of training that developers will be required to complete, it has not yet updated its training plan to reflect these new requirements. In addition, the Department has yet to require its developers to complete these required classes and reported that it plans to have all developers complete the required training classes by the end of December 2022.

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.

   Implementation in process—The Department approved its data classification procedures, which include guidance on how to classify its data, require developing a data classification inventory that is updated regularly, and specify requirements for protecting data based on its level of risk in April 2020. However, the Department has not updated these data classification procedures to include guidance on how the Department's confidential data should be processed on approved devices. Additionally, although the Department has continued to update and document its data classification inventory to categorize all its data sets at the application/system level, it has not yet completed the inventory/categorization for all of its data sets. The Department indicated it is working on a process for ensuring that only approved devices can access and process data and plans to finalize its procedures, complete the data inventory, and implement this recommendation by the end of December 2022.

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.

   Implementation in process—As indicated in our audit report, the Department has not conducted a formal Department-wide risk assessment since 2015; however, it has developed risk assessment training for using its new tools and templates for conducting a risk assessment, documenting the results, and prioritizing the areas in the Department's IT systems with the highest security risks for mitigation. The Department stated that it plans to update its risk assessment policy and procedures to provide guidance on using its new risk assessment tools and templates as well as complete a Department-wide risk assessment by the end of December 2022.

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.

   Implementation in process—The Department has continued to update and document its data classification inventory. However, it has not yet categorized all of its application/system-level data based on magnitude of harm and likelihood of risk. The Department also has yet to revise its risk assessment procedures to include categorizing the Department's information based on the likelihood of risk and magnitude of harm as required by ASET policy. The Department reported that it plans to revise and implement its risk assessment procedures by the end of December 2022.

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.

   Implementation in process—In April 2021, the Department updated its procedures to include processes for ensuring contractors, in addition to employees, comply with annual basic security awareness and HIPAA training requirements and acceptable use attestations. However, as indicated in the explanation for Recommendation 10, the Department has not yet determined its process for identifying the employees and contractors who should be required to complete role-based training. In addition, the Department has not yet updated its procedures to reflect its security awareness program and available training topic areas. The Department reported that it plans to revise and implement its security awareness procedures by the end of December 2022.

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

Implementation in process—The Department has finalized its role-based training matrix which indicates the specific roles, such as information security or data governance, that are required to take role-based training as well as the trainings and frequency of these trainings. However, some of the roles encompass broad categories of employees, such as all employees who define, create, or use data, and the Department has not developed a process for identifying the specific staff who will be required to complete each role-based training and tracking compliance with role-based training requirements. In addition, although the Department reported that some of its required role-based trainings were completed by applicable staff in 2020, other role-based trainings have yet to be offered. The Department plans to have all role-based trainings completed by applicable staff by the end of December 2022.

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.

Implementation in process—As of May 2021, the Department had awarded 3 grants since our initial followup. However, for 1 of the grants, the Department reported that it did not evaluate the grant applications using the electronic grants management system, although it indicated that all grants would be evaluated and awarded using the electronic grants management system. The Department reported that it planned to provide training on the electronic grants management system to applicable staff prior to posting and evaluating 2 new requests for grant applications to ensure consistency and transparency. However, when we contacted the Department in June 2022 for documentation to support that Department staff had received training and that the 2 new requests for grant applications were conducted using the electronic grants management system, the Department was unable to provide sufficient documentation indicating that staff had received the additional training and that the 2 new requests for grant applications were conducted using the electronic grants management system.

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.

Implementation in process—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. In addition, the policy requires Department staff who are responsible for providing support to its public bodies to also monitor and ensure compliance with open meeting law. We will continue to assess the Department's efforts to implement the open meeting law recommendations (Recommendations 12 through 14) during our 42-month followup.

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.

Implementation in process—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.

Partially implemented at 6 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 this 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.