## Auditor General's comments on Department response

The Joint Legislative Audit Committee requires all agencies to respond to whether they agree with our findings and plan to implement the recommendations. However, the Department has included certain statements in its response to the audit findings and recommendations that mischaracterize our work, attempt to minimize our work, or misdirect the reader from the message that the Department needs to improve its performance in various areas. To provide clarity and perspective, we are commenting on the Department's response to our audit.

1. The Department makes the following statements related to Finding 1 (see Department's response pages 2 and 3):

   "For example, in Finding 1, the report makes sweeping statements about public health and safety risks in the context of the auditors' review of 33 complaints and a judgmental sample of 37 self-reports for 5 long-term care facilities that are regulated and funded through an agreement with the federal Centers for Medicare and Medicaid Services (CMS). However, the audit fails to provide context for this analysis and findings. In total, long-term care facilities represent less than 0.5 percent of the total licensees under Department regulation and the sample of 5 facilities represents 0.014% of total licensees under the Department's jurisdiction. The complaints reviewed represent roughly 0.4% of all complaints received by the Department during the two-year period under evaluation. Rather than articulating how the Department performs across this wide range of activities to protect public health and safety and investigating and resolving complaints within its jurisdiction, the audit findings focus on this very narrow non-representative sample. In addition to only representing a small subset of the Department's overall regulatory activity, this sample is even small within the overall long-term care facility regulation framework, which received a total of 4,959 complaints over the two-year period in question."

   We disagree with the Department's characterizations. These statements are misleading, misrepresent the finding, and attempt to deflect attention from the Department's failure to investigate, or timely investigate or resolve, some long-term care facility complaints and self-reports. Specifically:

   a. Finding 1 does not include a sweeping statement regarding public health and safety, but instead clearly indicates that long-term care facility residents may be at risk because of the Department's failure to investigate, or timely investigate, some long-term care facility complaints and self-reports. In fact, the finding provides examples of complaints and self-reports from the sample we reviewed that include allegations of abuse and neglect and unsanitary living conditions that, if substantiated, either did or could put facility residents at risk. The failure to investigate these complaints or investigate them in a timely manner exacerbates this risk (see Finding 1, pages 7 through 15).

   b. Section headings and numerous sentences within the finding clearly discuss how our samples were selected and the specific results of those samples. For example, of the 147 long-term care facilities that are State licensed/CMS certified, we judgmentally selected 2 of the 5 facilities in our sample using information from a searchable database available through the Department's AZ Care Check website and CMS' website because of rating discrepancies in each facility's ratings on the 2 websites. Specifically, the Department's AZ Care Check website indicated that both facilities had been given an A rating, yet the CMS website indicated that the 2 facilities were rated overall as below average and much below average. We selected 3 facilities from a list of 39 facilities that had undergone and completed surveys (inspections) between December 2018 and May 2019 to ensure we captured

facilities from across the State within our sample. Specifically, of the 5 total facilities selected, 2 were Phoenix-area facilities, 1 was a Tucson facility, and 2 were facilities located in rural areas of the State (see Finding 1, footnote 10, page 8).

Although our test work was not designed nor intended to be generalized to the population of long-term care facilities, the methods we used to select and review complaints and self-reports provide reasonable assurance that the problems we identified are likely not limited to the facilities we reviewed. Furthermore, Department-provided data indicates that as of June 2019, 2,767 of the 4,958 long-term care facility complaints and self-reports the Department received in calendar years 2017 and 2018, or approximately 56 percent, remained open and uninvestigated (see Finding 1, page 9), consistent with our conclusion. The sample of complaints and self-reports we reviewed was sufficient, in the context of other evidence we provided in the report, to conclude that the Department did not timely prioritize and initiate some investigations on the complaints and self-reports it received against long-term care facilities (see Finding 1, pages 10 through 11).

2. The Department makes the following additional statements related to Finding 1 (see Department's response page 3):

"We would also note that under this federal program overseeing long-term care facilities, the Department performs functions for CMS, who sets the expectations, requirements and funding for the program. The Department is currently in compliance with those requirements as determined by CMS. The audit establishes expectations for the Department beyond those that exist in its agreement with CMS or as currently established by the Legislature, including establishing investigation time frames by examining policies in other states without a comprehensive analysis of those other states' requirements and available resources. If the State wants to expand the regulation of this industry beyond the federal requirements, including an evaluation of Arizona's long-term care marketplace and resources needed to meet any additional expectations that are set, the Department would be pleased to participate in those discussions. In summary, we will not detail every individual concern with how the audit articulates its findings. But as a result of these concerns, we cannot agree with Finding 1."

Similar to the Department's response noted in number 1 above, the Department includes statements in this portion of its response that misrepresent its compliance with CMS requirements and expectations regarding its performance related to investigating long-term care facility complaints and self-reports. Specifically:

a. Although the Department indicates that CMS has determined it is in compliance with CMS requirements for overseeing long-term care facilities, as indicated in our report, the Department is not meeting all CMS requirements. The Department is federally required to investigate all complaints and self-reports and prioritize and initiate investigations of those complaints and self-reports in a timely manner. As presented in Finding 1, as of June 2019, 38 of the 70 complaints and self-reports in our sample, or 54 percent, remained uninvestigated between 173 and 904 days after receipt. We also identified deficiencies with timely prioritizing and initiating investigations in accordance with CMS requirements for the complaints and self-reports in our sample, similar to CMS findings. Specifically, as indicated in our report, according to the Department's 4 annual CMS State Performance Evaluations for federal fiscal years 2015 through 2018, the Department did not always meet the federal time frame for initiating its complaint and self-report investigations (see Finding 1, pages 9 through 11, and 13).

b. Performance audits provide findings and recommendations to help management improve program performance and operations. These recommendations should not be limited to what is required only by State or federal laws and regulations, but include recommendations to help improve performance and protection of the public health and safety—and in this case, residents of long-term care facilities. As a result, our report provides meaningful, common-sense recommendations, such as establishing a time frame for completing investigations or developing and implementing additional management reports for Department management review and analysis that will help ensure that all complaints and

self-reports are prioritized, investigated, and resolved in a timely manner (see Finding 1, page 14). In addition, we include information on other states when appropriate to provide helpful benchmarking information for the audited agency, policymakers, and other users of our performance audit reports. As indicated in Appendix A of our report (see page a-1), we researched whether 11 western states had complaint-handling time frames and identified 1 state, California, that statutorily requires complaint investigations to be completed within 60 days of receipt (see Finding 1, page 10).

3. The Department makes the following statements related to Finding 3 (see Department response pages 3 through 4):

"The Department also cannot agree with Finding 3. We take seriously our obligation to protect critical, sensitive and confidential data. ADOA-ASET is the Arizona office responsible for setting the technology, security, privacy, and communication strategies, policies, and procedures for the state of Arizona. ASET's guiding principles include *Driving best-in-class, enterprise-wide security standards through the office of the state Chief Information Security Officer (CISO) in an effort to ensure that all cyber security initiatives are secure and compliant*. To this end, ASET provides leadership, standards and governance across all of state government, leveraging its experts to set expectations and monitor enterprise security controls and state agency activities. The report misrepresents our IT security processes, including using inaccurate terminology to describe activities in the report (e.g., use of the term "breach", which did not occur, but was implied to have occurred in the report). The incident referenced in the audit involved a multistep, complicated process in which an individual would have needed specific knowledge to access the information. Contrary to what is reported in the audit, ADHS's web application development policies and procedures are aligned with ASET and credible industry standards."

"In addition, the audit reports that the Department has not conducted a formal Department-wide IT risk assessment since 2015. This misleading statement fails to explain that ASET conducted a state-wide risk assessment several years ago and determined that Arizona could greatly reduce IT risks by implementing enterprise controls. The Department and other states agencies have focused on implementing these controls over the past few years, including the establishment of RiskSense, a tool used for IT vulnerability management and risk scoring. The RiskSense platform includes the assignment of a safety score which is used to evaluate and monitor each agency's risk exposure. Governor Ducey and ASET set a goal for each state agency to maintain a score of 725 or above; the Department currently exceeds this goal. In addition, the score is updated at least twice a month and Department leadership reviews its performance weekly and allocates resources as needed to address identified issues. Now that these controls have been implemented, the Department plans to return to performing annual risk assessment. The Department believes ASET provides sufficient and appropriate leadership on IT security issues and will continue to work collaboratively with ASET to maintain its agency's information security. It will also implement recommendations that will continue to enhance its procedures."

We disagree with some of the Department's statements included in the above portion of its response. They are inaccurate or are an attempt to minimize the importance of our findings and recommendations that are provided to help improve the Department's processes for safeguarding critical, sensitive, and confidential data and reduce the risk of unauthorized access to this data. Specifically:

a. The Department states that by using the term "breach" in Finding 3, our report implies that a breach occurred. This statement misrepresents our finding in this area. We use the term "breach" to explain a statutory requirement relating to the unauthorized access of confidential data, not to describe the incident. Specifically, statute states that it is a class 1 misdemeanor for any person, including an employee or official of the Department or another State agency or local government, to breach the confidentiality of this information. However, in discussing the unauthorized access that occurred, we refer to it as a security weakness and a security incident, not a breach. Similarly, based on its own investigation of what we found and reported to the Department, the Department used similar language in reporting that a security incident had occurred (see Finding 3, pages 21 through 22).

b. The Department indicates that the security incident we report involved a multistep, complicated process. We disagree. Obtaining access to the information involved only a few steps, including a common step that an attacker would initiate. Specifically, as stated in the report, a concerned member of the public informed us of the security weakness on a Department website that allowed them unauthorized access to statutorily confidential data. Based on the information provided, we were able to obtain unauthorized access, and it was not complicated to do so. Additionally, the Department's response downplays the significance of the security weakness found during the audit.

c. The Department indicates that its web application development policies and procedures are aligned with ASET and credible industry standards. We disagree. Based on the documents the Department provided for our review and as indicated in our report, its policies and procedures are not aligned with ASET and credible industry standards because they do not require gathering security requirements, using up-to-date secure coding standards, performing threat modeling during web application development, and performing security testing (see Finding 3, page 22).

d. The Department indicates that our statement regarding when it last conducted a formal Department-wide risk assessment is misleading. However, based on the documents and information the Department provided, we accurately report that the Department has not performed a Department-wide risk assessment since 2015. In addition, despite other activities the Department is performing as mentioned in its response, ASET policy requires the Department to conduct a Department-wide risk assessment at least annually (see Finding 3, pages 23 through 24).

4. Finally, as indicated in its response, the Department also does not plan to implement recommendations 5 and 6 from our report (see Department response page 7).

We disagree with the Department's determination to not implement recommendations 5 and 6. By not taking steps to implement these recommendations, the Department will not be doing everything it can and/or is required by ASET policy to safeguard its IT systems and data, thus increasing the risk of inappropriate or unauthorized access to these systems and data. Specifically, Recommendation 5 focuses on requiring its web application development staff to receive regular role-based training. Although its staff have received training, by not requiring its staff to regularly receive role-based training, the Department risks its staff not being up to date on secure coding practices or IT security threats. Recommendation 6 focuses on updating its data classification policies and procedures to provide guidance on how to classify its data and creating and updating a data classification inventory, as required by ASET and recommended by credible industry standards. As indicated in our report, data classification helps to ensure sensitive data is protected from loss, misuse, or inappropriate disclosure (see Finding 3, page 23).