COMMITMENT
INTEGRITY
LEADERSHIP

July 16, 2019
Report 2018-611
FACT SHEET

Elaine M. Howle *State Auditor*

CONTACT: *Margarita Fernández* | *(916) 445-0255 x 343* | *MargaritaF@auditor.ca.gov*

Gaps in Oversight Contribute to Weaknesses in the State's Information Security

High Risk Update—Information Security

Background

Our office previously reported on the deficiencies we identified in security controls that state agencies—under the oversight of the California Department of Technology (technology department)—have implemented over their information systems. The pervasiveness of these deficiencies led us to designate, in 2013, information security as a high-risk issue. The technology department is responsible for providing direction for the State's information security and protecting the State's information assets. It creates, issues, and maintains security standards that provide the security and privacy policy framework with which state entities under the direct authority of the governor (reporting entities) must comply. In 2015, we reported that many state entities' information assets were potentially vulnerable to attack or disruption. We also observed that a significant number of entities—such as constitutional offices and those in the judicial branch—are not subject to the technology departments' security standards (nonreporting entities).

Our Key Recommendations

The Legislature should amend state law to require nonreporting entities to do the following:

- Adopt information security standards comparable to those reporting entities must adopt.
- Obtain or perform comprehensive information security assessments no less frequently than every three years.
- Confidentially submit certifications of their compliance with their adopted standards and, if needed, corrective action plans to address any outstanding deficiencies to the Legislature.

Key Findings

- Gaps in oversight weaken the State's efforts to keep its information secure. In fact, most of the 33 nonreporting entities that we surveyed are not adequately addressing information security.
  - » Four entities had not performed an information security assessment and thus, may be unaware of whether their controls are implemented correctly and operating as intended, and three of those entities had no current plans to proceed with an assessment.
  - » Twenty-four of 29 entities that had obtained an information security assessment learned they were only partially compliant with their selected standard.
- Although aware of significant deficiencies in their current information security programs, some nonreporting entities have been slow to address these weaknesses—two of the 24 nonreporting entities with partial compliance asserted that they had resolved their high-risk deficiencies while 11 stated that they needed an additional three years to resolve them.
- The majority of nonreporting entities we reviewed have not taken steps to develop and document a comprehensive understanding of their information security status and thus, may not know if they are properly protecting their information assets against unauthorized access, use, disclosure, disruption, modification, or destruction.
- Most of the nonreporting entities do not have an external oversight framework that would require them to assess their information security regularly.