COMMITMENT
INTEGRITY
LEADERSHIP

January 18, 2022
Report 2021-602
FACT SHEET

Michael S. Tilden *Acting State Auditor*

CONTACT: *Public Affairs Office* | *(916) 445-0255*

State High-Risk Update—Information Security

The California Department of Technology's Inadequate Oversight Limits the State's Ability to Ensure Information Security

Background

Information security breaches and shutdowns of information systems and critical infrastructure have affected retailers, financial institutions, and government agencies in recent years. Such incidents highlight the importance of protecting the State's information. The California Department of Technology (CDT) is responsible for providing direction for the State's information security. State entities within the executive branch that are under the Governor's direct authority must comply with the information security and privacy policy standards that CDT issues and maintains. Although CDT plays a critical role in advising such entities on security issues and helping to ensure their compliance with state policy, entities are ultimately responsible for their own information security.

Key Findings

CDT does not have a complete status of the State's information security—it has been slow to assess the information security development of high-risk entities through its oversight life cycle and has failed to proactively expand its capacity to do so.

CDT does not utilize much of the self-reported information available to it from the entities it oversees, which it could use to help inform the overall status of the State's information security and to identify common areas that require improvement across the State.

The information that CDT has collected indicates that entities under its purview continue to perform below recommended standards.

CDT does not provide adequate transparency to the Legislature on the status of the State's information security deficiencies.

CDT has failed to complete timely updates to ensure that its policies align with the federal information security standards, and its guidance related to the security of personal devices used for teleworking is not entirely clear.

Although many state entities that fall outside of CDT's oversight authority have adopted an information security framework or standards, few have achieved full compliance with it.

Some entities that are not subject to CDT's oversight do have an external oversight framework that requires them to assess their information security regularly, and we previously found that such entities were generally further along in their information security development than those without the external oversight.

Key Recommendations

To strengthen the information security practices of all state entities, the Legislature should amend state law so that it requires CDT to confidentially submit an annual statewide information security status report to the appropriate legislative committees. The Legislature should also require each state entity not overseen by CDT to do the following:

- Adopt information security standards comparable to those of state entities overseen by CDT.
- Provide annual status updates to legislative leadership on their compliance with the standards.
- Perform or obtain audits of their information security at least every three years.

To ensure that CDT understands the statewide security status of entities under its purview, it should increase its capacity to perform timely compliance audits of high-risk entities, which may entail hiring more staff or securing additional contracted audit support. CDT should also do the following:

- Use information from the various self-assessments that applicable entities complete to help identify systemic issues.
- Complete the necessary updates to the State's information security and privacy policies to ensure that entities are aware of new federal information security standards.
- Clarify guidance for teleworking employees using personal devices for state business.