COMMITMENT
INTEGRITY
LEADERSHIP

April 20, 2023
Report 2022-114

FACT SHEET

Grant Parks *California State Auditor*

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

California Department of Technology

Weaknesses in Strategic Planning, Information Security, and Project Oversight Limit the State's Management of Information Technology

Background

Over the past two decades, California has experienced significant challenges related to its information technology (IT) infrastructure, including failed IT projects that cost the State hundreds of millions of dollars, system outages that left Californians unable to access critical services, and inefficiencies resulting from outdated technology that likely have resulted in frustration and misgivings about government effectiveness. State law and policy give the California Department of Technology (CDT) responsibility for and broad authority over nearly all aspects of IT in state government. Specifically, CDT must produce an annual IT strategic plan to guide the State's acquisition, management, and use of IT. In addition, state law requires CDT to issue and maintain policies governing the State's information security and gives CDT the authority to conduct independent security assessments of every state agency. Finally, CDT is responsible for providing oversight of the State's IT projects. It has the authority to approve, suspend, terminate, and reinstate IT projects.

Key Findings

- CDT's statewide IT strategic plan does not include measurable objectives, such as a description of specific tasks or timelines necessary to achieve the plan's broad goals.
  - » CDT's plan does not include performance measures that CDT would use to evaluate progress.
  - » CDT has identified a need for qualified and experienced IT staff in state service, but it did not identify in the plan any specific actions or initiatives to address this need.
- CDT has yet to fully assess the overall status of the State's information security.
  - » Information CDT has obtained indicates that most reporting entities are not making significant progress toward improving their information security.
  - » CDT will likely not be able to complete audits for all reporting entities until June 2030.
- CDT did not always adequately intervene in the projects we reviewed to ensure that the agencies resolved the problems that its project oversight identified.
  - » CDT could not provide evidence that it had used its suspension, reinstatement, or termination authority for any project since 2016.
  - » CDT did not use its authority to require any of the agencies for the four projects we reviewed to develop a corrective action plan to get their IT projects back on track, even when the projects exhibited conditions that should have necessitated corrective action.
- Under the State's current structure for IT project oversight, CDT's independence is compromised, limiting the effectiveness of its efforts.

Key Recommendations

The Legislature should require CDT to do the following:

- Develop measurable objectives to achieve IT strategic plan goals, incorporate performance measures for those objectives, and monitor the State's progress toward achieving the plan's goals.
- Create and lead an interorganizational task force to assess IT staffing problems in the State and to issue recommendations to increase the State's hiring and retention rates of highly qualified IT personnel.
- Develop a plan for determining the overall statewide information security status of the State's reporting entities by January 2024.

The Legislature should create a new board or committee to improve the independence of the State's IT project oversight.