FACT SHEET

Elaine M. Howle State Auditor

CONTACT: Margarita Fernández | (916) 445-0255, x343 | MargaritaF@auditor.ca.gov

The California State Auditor released the following report today:

High Risk Update—Information Security

Many State Entities' Information Assets Are Potentially Vulnerable to Attack or Disruption

BACKGROUND

Our office previously identified the California Department of Technology's (technology department) oversight of general controls state agencies have implemented over their information systems as a high risk issue. The technology department serves as the primary state government authority for ensuring the confidentiality, integrity, and availability of state systems and applications for certain executive branch entities. Further, it is responsible for providing statewide strategic direction and leadership in the protection of the State's information assets and thus has created 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.

KEY FINDINGS

During our audit of the technology department's oversight of the State's information security, we noted the following:

- Most reporting entities—including some that maintain sensitive or confidential information—have poor controls over their information systems and are not fully compliant with the information security and privacy policies, standards, and procedures.
  - ✓ Only four of the 77 respondents to our survey of reporting entities stated that they had fully complied with all of the security standards—many have not developed comprehensive inventories of their information assets and have not identified their information security risks.
  - ✓ We found deficiencies in each of the five reporting entities we reviewed—one of the entities had only partially complied in two of the five control areas we reviewed and had not yet addressed the other three control areas.
  - ✓ Most reporting entities have not adequately planned for interruptions or disasters—only 23 of the 77 survey respondents stated they have fully met technology recovery plan requirements and three of the five entities we visited have only partially met those requirements.
- The technology department has not provided effective oversight or guidance to reporting entities and thus cannot ensure the confidentiality, integrity, and availability of some of the State's most critical information and information systems.
  - ✓ It was unaware that many reporting entities have deficiencies in their information security—37 of the 41 survey respondents that certified compliance to the technology department in 2014 were actually noncompliant.
  - ✓ It has allowed some entities' weaknesses to persist for years—we identified 18 reporting entities that either self-certified that they were not fully compliant or did not have a certification form on file for at least five years.
  - ✓ Thirty of the 38 survey respondents that certified noncompliance in 2014 indicated that they submitted remediation plans but only four stated that the technology department followed-up on those plans.
- Some state entities—judicial branch entities, constitutional offices, and certain executive branch entities—are not subject to the security standards or the technology department's oversight and yet we have reported significant deficiencies in control over some of those entities' information systems in the past.

KEY RECOMMENDATIONS

We recommended that the Legislature mandate that the technology department conduct a security assessment of each reporting entity at least every two years and authorize it to redirect funds if available to remediate information security weaknesses. To the reporting entities, we recommended that they develop remediation plans for the noncompliant areas.

Further, we made numerous recommendations to the technology department, including the following:

- Develop a self-assessment tool that reporting entities can use to determine their level of compliance with standards; provide extensive guidance and training on the standards and self-assessment tool; develop policies and procedures for reviewing self-assessments and self-certifications; and annually follow-up on remediation plans.
- Provide more effective oversight and develop an ongoing risk-based audit program for site visits; and improve the clarity of the security standards by regularly reaching out to reporting entities to gain their perspective, make improvements, and develop training.

Date: August 25, 2015 **Report: 2015-611**