A JOINT OVERSIGHT HEARING OF THE ASSEMBLY COMMITTEE ON PRIVACY & CONSUMER PROTECTION AND SELECT COMMITTEE ON CYBERSECURITY

STATE AUDITOR REPORT "GAPS IN OVERSIGHT CONTRIBUTE TO WEAKNESSES IN THE STATE INFORMATION SECURITY, HIGH RISK UPDATE – INFORMATION SECURITY"

August 13, 2019
1:30 p.m.
State Capitol, Room 126

BACKGROUND PAPER

I. Background

In July 2019, the Auditor of the State of California released a report titled "*Gaps in Oversight Contribute to Weaknesses in the State's Information Security"* (hereinafter "Report"). The Report provides critical insight into information security standards utilized by various state agencies in California and provides a series of recommendations by which these particular agencies may improve their information security.

On Tuesday, August 13, 2019, the Assembly Committee on Privacy & Consumer Protection and Assembly Select Committee on Cybersecurity, in consultation with the Joint Legislative Audit Committee, will hold an oversight hearing to hear from a number of panelists with expertise in information security and government. In doing so, the Committees will hear directly from the State Auditor's office regarding its audit, as well as from the California Department of Technology (CDT) regarding its experiences and responses to various findings and recommendations in the audit. Notably, this Background Paper is not intended to duplicate the recent work of the Auditor, but to instead summarize the history of statutory information security requirements and specific legislative efforts preceding the Auditor's findings. (The full Report may be found online at <http://www.bsa.ca.gov/pdfs/reports/2018-611.pdf> [as of Aug. 11, 2019].)

In holding these discussions around the findings and recommendations of this recent Report, the Committees intend to explore the following questions, among others:

- Would the jurisdictional authority of constitutional offices and other nonreporting entities be impeded or otherwise hindered if required by the Legislature to follow the statewide standards set by an executive branch entity under the direction of the Governor? If so, how?

- Would nonreporting entities benefit overall from the information security expertise provided by the Executive Branch? What would be the advantages or disadvantages?

- Do the constitutional offices and other nonreporting entities that were the subject of the Report have sufficient information security expertise and capabilities to operate independently from the remainder of the Executive Branch, which is otherwise subject to the information security standards and assessments mandated under Government Code Section 11549.3?

- Are there certain constitutional entities that have unique information security needs or circumstances that warrant an exemption from the Office of Information Security (OIS) standards and information security assessments (ISAs)?

- Does effective oversight of information security require specific technical expertise? Is that expertise generally held by the constitutional offices and other nonreporting entities that are the subject of the Report?

- How do the ISAs conducted by the OIS or the California Military Department compare to the ISAs conducted by private vendors?

- How might reporting to CDT with respect to information security jeopardize nonreporting entities' independence, if at all? Are any of those same entities subject to other CDT authority (such as in the realm of information technology (IT) project oversight) or the authority of other Executive Branch entities in other respects?

- What are the functional differences between the International Organization for Standardization and the International Electrotechnical Commission 27000 family of standards (ISO/IEC 27000 family), National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) and California's *State Administrative Manual* (SAM) information security standards?

- Would adopting one standard over another significantly impact the information security of the State? Would the overall cybersecurity posture of the State benefit from applying the

same standards across California State government, or is the posture unaffected as long as one of the aforementioned standards is utilized?

- Assuming any of the three aforementioned standards are acceptable for compliance by nonreporting entities, given that each of these standards are updated and controlled by a standards organization, what (if any) standards followed by nonreporting entities need to comply with the most recently updated standard?

- CDT has created a cybersecurity maturity metric that is intended to allow for direct comparisons of a variety of state entities by using SAM required assessments and audits. Would requiring nonreporting entities to follow a maturity metric created by the Executive Branch for the purposes of evaluating statewide cybersecurity maturity be problematic?

II. General history of IT oversight in California State Government and statutory definitional issues giving rise to the current "gap"

In recent decades, California has used various models to manage and oversee IT and information security in state government. Issues or controversies surrounding an IT project or contract, or the beginning of a new gubernatorial administration have typically preceded the changes in these models. What is today the California Department of Technology (CDT) under the Government Operations Agency, was previously the California Technology Agency (CaTA), the Office of the State Chief Information Officer (OCIO), and the California Department of Information Technology (DOIT), with a significant gap between the demise of DOIT (2002) and the creation of the OCIO (2006) in which the State lacked any centralized IT office. With each new iteration of statewide IT oversight, the purview of the new entity has expanded or contracted in different areas to respond to the cause of the reorganization.

These contractions and expansions, in the form of centralizing IT functions or federating responsibilities to individual agencies in the absence of a centralized IT office, have sometimes made it difficult to determine who is responsible or accountable for certain functions, including information security. Certainly, the process of revising and recasting similar functions in State government over the years has, as a practical matter, left a statutory system in the Government Code that is, at times, difficult to follow. Most relevant to this hearing is how the Government Code applies different terms such as "state agency" and "state entity," among others, to arguably reference the same concept, often at times within the same code section despite competing definitions for those terms. The Report highlights how the applicability of information security standards for state agencies largely rests on such terms used in Government Code Section 11549.3. Throughout Section 11549.3 (which establishes the OIS and its responsibilities within CDT), the terms "state agencies," "state entity," "state agency, department, or office," and "all state entities defined in Section 11546.1" are used in various provisions to describe the focus of

the OIS. That being said, it is largely unclear why a particular term is used at times in one provision in lieu of an alternative term used in surrounding provisions.

What is clear, however, is that the phrase "all state entities defined in Section 11546.1" is narrower than the term "state agency" or the term "state entity" more generally, because Section 11546.1 limits that term to those entities that are "under the direct authority of the Governor". Of course, there are many state entities, even within the Executive Branch, that are not under the Governor's direct authority. In contrast, the term "state agency" when not specifically defined in a particular context, is defined by Section 11000 of the Government Code to "include[] every state office, officer, department, division, bureau, board, and commission" except the California State University, unless the section explicitly provides that it applies to the university.

The difference between these two terms, in the instance of information security, is critical. The phrase "all state entities defined in Section 11546.1" determines which agencies or entities must follow the information security requirements created by OIS pursuant to subdivision (b) of Government Code Section 11549.3. Notably, the phrase does not, however, expressly determine the "state entities" subject to ISAs under subdivision (c) of that same section – though some nonreporting entities have reportedly disagreed with this interpretation of the law. Indeed, these ambiguities have been of particular interest to the Legislature over the past few years as it has sought to respond to evolving threats to the State's IT networks and the growing prominence of cybersecurity as a critical function for all organizations. Specifically, the Legislature has sought to clarify (and at times reassert) the roles of certain actors within State government.

For example, AB 670 (Ch. 518, Stats. 2015) was drafted *without* using the narrower phrase identified above, recognizing the need for the entire State government to undergo the fundamental practice of an ISA. However, as discussed above, certain constitutional offices maintain that the requirement (codified at Section 11549.3(c)) does not impact them because of the narrow use of the phrase "state entity" in the preceding subdivision (Section 11549(b)).

Recognizing this ongoing problem, AB 3193 (Chau et al, 2018), jointly authored by the Chairs of these Committees and Assemblymember Obernolte, sought to bring clarity and accountability to nonreporting entities by removing the limiting definitional reference in Section 11549.3(b) and making clear that *all* "state agencies" (which, consistent with the Section 11000 definition includes nonreporting entities) must follow certain information security standards. The bill failed in the Senate Committee on Governmental Organization after numerous constitutional offices opposed the measure. The same opposition was raised to AB 1242 (Irwin, 2019) which included this same proposal, among other things. Writing in opposition to that bill, the State Controller wrote "[the State Controller's Office] has lived up to the commitment to meet or exceed the standards established by law. As a result, I do not see what problem AB 1242 seeks to solve." These Committees may, however, have reason to question whether the stated voluntarily compliance of constitutional offices with various legal standards is sufficient or if private vendor ISAs may be adequately relied upon to demonstrate compliance, given that the Report indicates

both issues of partial compliance with selected information security standards by a majority of those nonreporting entities reviewed and a concern over whether nonreporting entities are even fully aware of all the possible weaknesses in their information security, among other issues. (*See* Report, p. 9.)

Despite such efforts to bring information security standardization to "nonreporting entities," or entities that are not under the Governor's direct authority, such as constitutional offices and the judicial branch, these nonreporting entities still operate largely without oversight. Given recent oversight hearings by these Committees indicating that the State has made significant progress in the area of cybersecurity through the coordinated efforts of CDT (and particularly OIS) with its cybersecurity partners (the Office of Emergency Services, the California Highway Patrol, and the California Military Department; together, the State's "four core cybersecurity partners"), it raises a question as to whether maintaining a siloed (as opposed to uniform) approach to information security is sustainable or the most secure approach to take across State government.

While the specific nonreporting entities that are the subjects of the Report are unnamed and have been kept confidential for security reasons, the Auditor's findings and recommendations show that, at minimum, nonreporting entities need to do more to safeguard the information they collect, maintain, and store. The Report strongly suggests that, as a whole, the information security practices of nonreporting entities would benefit from consistent oversight. This hearing was organized in anticipation of the need to address these issues with future action, including potential legislation.

III. Report's recommendations

For reference, the Report concludes with the following recommendations to the Legislature:

> To strengthen the information security practices of nonreporting entities, the Legislature should amend state law to do the following:
>
> - Require all nonreporting entities to adopt information security standards comparable to SAM 5300.
>
> - Require all nonreporting entities to obtain or perform comprehensive information security assessments no less frequently than every three years to determine compliance with the entirety of their adopted information security standards.
>
> - Require all nonreporting entities to confidentially submit certifications of their compliance with their adopted standards to the Assembly Privacy and Consumer Protection Committee and, if applicable, to confidentially submit corrective action plans to address any outstanding deficiencies. (*See* Report, p. 16.)