Date of Hearing: April 19, 2022

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
AB 2135 (Irwin) – As Amended April 7, 2022

SUBJECT: Information security

SUMMARY: This bill would require state agencies that do not fall under the direct authority of the Governor to adopt and implement certain information security and privacy policies, standards, and procedures meeting specified federally-established criteria, and would require those agencies to perform a comprehensive independent security assessment (ISA) every two years for which they may contract with the Military Department or a qualified responsible vendor. Specifically, **this bill would**:

1) Require every state agency not subject to the information security and privacy standards, practices, and procedures issued by the Office of Information Security (OIS), i.e. agencies that do not fall under the direct authority of the Governor, to adopt and implement information security and privacy policies, standards, and procedures that adhere to specified federal standards.

2) Require every state agency described in 1), above, to conduct an ISA every two years in order to assess all policies, standards, and procedures adopted pursuant to 1), as applicable.

3) Permit a state agency described in 1), above, to adopt and implement the information security and privacy policies, standards, and procedures established by OIS in order to satisfy the requirement prescribed by 1), and permit a state agency to discontinue a policy, standard, or procedure electively adopted as such at any time.

4) Permit a state agency described in 1), above, to contract with the Military Department, or with a qualified responsible vendor, to perform an ISA pursuant to 2), above, and specify that the cost of the ISA shall be funded by the agency being assessed.

5) Require every state agency described in 1), above, to certify by February 1 annually to legislative leadership, consisting of the President pro Tempore of the Senate and the Speaker of the Assembly, that the agency is in compliance with all policies, standards, and procedures adopted pursuant to the bill; and specify that the certification shall include a risk register and plan of action and milestones in accordance with the criteria specified in the Statewide Information Management Manual (SIMM).

6) Specify that, notwithstanding any other law, the certification made pursuant to 5), above, shall be kept confidential and shall not be disclosed, except that the information and records may be shared, maintaining a chain of custody, with the members of the Legislature and legislative employees, at the discretion of either the President pro Tempore of the Senate or the Speaker of the Assembly.

7) Require Legislative leadership, or their designee, to consult with the state agencies described in 1), above, on the policies and procedures for transferring, receiving, possessing, or disclosing certifications that ensure confidentiality and security of the certification, and to determine the form required for the certification.

EXISTING LAW:

1) Establishes, within the Government Operations Agency, the Department of Technology (CDT), and generally tasks the department with the approval and oversight of information technology (IT) projects, and with improving the governance and implementation of IT by standardizing reporting relationships, roles, and responsibilities for setting IT priorities. (Gov. Code Sec. 11545, et seq.)

2) Establishes, within the CDT, the Office of Information Security (OIS), with the purpose of ensuring the confidentiality, integrity, and availability of state IT systems and promoting and protecting privacy as part of the development and operations of state IT systems, and tasks OIS with the duty to provide direction for information security and privacy to state government agencies, departments, and offices. (Gov. Code Sec. 11549(a) and (c).)

3) Requires the chief of OIS to establish an information security program with responsibilities including, among others, the creation, updating, maintenance, and issuing of information security and privacy policies, standards, and procedures for state agencies, and of policies, standards, and procedures directing state agencies to effectively manage security and risk for IT, and for mission critical, confidential, sensitive, or personal information. (Gov. Code Sec. 11549.3(a).)

4) Establishes comprehensive information security and privacy policies, standards, and procedures for state agencies, including guidelines for risk management and assessment. (State Administrative Manual Sec. 5300, et seq.)

5) Authorizes OIS to conduct, or require to be conducted, an ISA of every state agency, department, or office, the cost of which shall be funded by the state agency, department, or office being assessed, and specifies that OIS must, in consultation with the Office of Emergency Services, annually require no fewer than 35 state entities to perform an ISA. (Gov. Code Sec. 11549.3(c)(1) and (2).)

6) Authorizes the Military Department to perform an ISA of any state agency, department, or office, the cost of which shall be funded by the agency, department, or office being assessed. (Gov. Code Sec. 11549.3(c)(3).)

7) Specifies that, notwithstanding any other law, during the process of conducting an ISA, information and records concerning the ISA are confidential and shall not be disclosed, except to state employees or contractors who have been approved as necessary to receive the information and records to perform the ISA or subsequent remediation activity, and that the results of a completed ISA are subject to all applicable laws relating to disclosure and confidentiality including the California Public Records Act. (Gov. Code Sec. 11549.3(f).)

8) Provides that nothing in the California Public Records Act shall be construed to require the disclosure of an information security record of a public agency, if, on the facts of the particular case, disclosure of that record would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency. (Gov. Code Sec. 6254.19.)

9) Provides that a state entity's information security program shall incorporate an Information Security Program Plan (ISPP) to provide for the proper use and protection of its information

assets, including a Risk Register and Plan of Action and Milestones (POAM) process for addressing information security program deficiencies; and provides detailed instructions and a standardized form for completing a Risk Register and POAM. (State Information Management Manual Sec. 5305, et seq.)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of this bill**: This bill seeks to enact recommendations of the California State Auditor to resolve weaknesses in the State's information security by ensuring that all state agencies, including those that do not fall under the direct authority of the Governor, implement comprehensive information security and privacy standards and practices, and are subject to regular security assessments and oversight. This bill is author sponsored.

2) **Author's statement**: According to the author:

> Due to the various definitions of the terms "state agency" and "state entity" along with other references to subsidiary forms of the State, there is a lack of uniformity of who must follow cybersecurity-related statutes, including standards created by CDT's Office of Information Security (OIS) for the protection of the State. Some state entities, most prominently Constitutional Officers, argue that they are not covered by the statutes, and their constitutional independence makes it untenable to report to CDT about their compliance with any standards, including ones on information security. […]
>
> This legal stance results in a handful of state entities having no measurable accountability when it comes to cybersecurity. This lack of accountability was identified and lamented by the State Auditor, when they reviewed the cybersecurity posture of non-reporting entities and found them to be in far worse condition than reporting entities, who have shown some progress towards improved security over multiple audits […]. This disconnect between different types of state entities further creates the possibility that these entities are spending time and funds on parallel structures to develop, implement, and monitor cybersecurity standards within their own network, instead of utilizing the existing resources provided by CDT.

3) **State investments in cybersecurity**: According to the Federal Bureau of Investigation's Internet Crime Complaint Center (FBI IC3) 2021 report, California leads the nation by a staggering margin in both the number of victims of internet crime and in the estimated costs experienced by the victims, with nearly 50% more victims and over twice the costs compared to the next closest states, respectively.[1] Acknowledging the pressing cybersecurity issues facing this State and, in particular, the State's public agencies, California has in recent years invested heavily in the security of its IT infrastructure.

   Of relevance to this bill, in 2010, the Legislature passed AB 2408 (Smyth, Ch. 404, Stats. 2010), which, among other things, required the chief of OIS to establish an information

---

[1] Internet Crime Complaint Center, "Internet Crime Report 2021," *Federal Bureau of Investigation*, Mar. 22 2022, https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2021-internet-crime-report, [as of Apr. 9, 2022].

security program, with responsibilities including the creation, updating, maintenance, and issuing of information security and privacy policies, standards, and procedures for *state agencies*, and of policies, standards, and procedures directing *state agencies* to effectively manage security and risk for IT and for mission critical, confidential, sensitive, or personal information. (Gov. Code Sec. 11549.3(a).) AB 2408 provided that all *state entities* shall implement the policies and procedures issued by OIS, including compliance with its information security and privacy policies, standards, and procedures, and with filing and incident notification requirements. (Gov. Code Sec. 11549.3(b).) Five years later, the Legislature expanded on the authority of OIS by passing AB 670 (Irwin, Ch. 518, Stats. 2015), which authorized OIS to conduct, or require to be conducted, an ISA of every *state agency, department, or office*, at the expense of the entity being assessed, and specified that OIS must, in consultation with Cal OES, annually require no fewer than 35 *state entities* to conduct an ISA. (Gov. Code Sec. 11549.3(c)(1) and (2).) AB 670 allowed these ISAs to be conducted by the Military Department, which serves a principal role on Cal-CSIC and houses the Cyber Network Defense (CND) unit, a division with the goal of "assist[ing] agencies by providing actionable products, assistance, and services designed to improve overall cybersecurity compliance, reduce risk, and protect the public." (Gov. Code Sec. 11549.3(c)(3).)

Although AB 2408 and AB 670 were fairly prescriptive in assigning responsibilities to OIS and in mandating state agencies/entities to comply with the standards and practices set forth by OIS, the juxtaposition of the terms "state agency" and "state entity" has created significant problems for statutory interpretation, especially in the context of neighboring statutes in the Government Code. The confusion stemming from the inconsistent uses of these terms has raised questions as to which agencies are subject to the provisions of AB 2408 and AB 670, resulting in critical gaps in the cybersecurity of some state networks. AB 2135 seeks to clarify the applicability of information security oversight and responsibilities laid out by AB 2408 and AB 670, and to ensure these gaps in state cybersecurity are appropriately resolved.

4) **"State agency" vs. "state entity"**: Under existing law, the Government Code's default definition for "state agency" includes every state office, officer, department, division, bureau, board, and commission, except the California State University, unless a specific definition is given otherwise. (Gov. Code Sec. 11000.) By and large, provisions pertaining to CDT use the term "state agency" without providing a specific definition, and thus this default definition typically applies. In various provisions relating to CDT, the term "state entity" also appears, but is defined only in a single instance (Gov. Code Sec. 11546.1(e)), with that definition cross-referenced in another single instance (Gov. Code Sec. Section 11549.3(b)). In those instances, "state entity" is defined to mean "an entity within the executive branch that is under the direct authority of the Governor, including, but not limited to, all departments, boards, bureaus, commissions, councils, and offices *that are not defined as a 'state agency' pursuant to paragraph (1).*" (Gov. Code Sec. 11546.1(e)(2); emphasis added.) Paragraph (1) defines "state agency" in that instance to mean "the Transportation Agency, Department of Corrections and Rehabilitation, Department of Veterans Affairs, Business, Consumer Services, and Housing Agency, Natural Resources Agency, California Health and Human Services Agency, California Environmental Protection Agency, Labor and Workforce Development Agency, and Department of Food and Agriculture." (Gov. Code Sec. 11546.1(e)(1).)

In the statute established by AB 2408, OIS is tasked with developing an information security program and, among other things, establishing policies, standards, and procedures directing *state agencies* to effectively manage security and risk. (Gov. Code Sec. 11549.3(a)(2).) However, in the very next subdivision, the same statute indicates that "all *state entities* defined in Section 11546.1" must comply with those information security policies, standards, and procedures. That cross-reference is to the aforementioned definition for "state entity," which provides an unusually narrow definition for the term "state entity," and resides in an entirely different chapter of the code relating to CDT's project oversight and other non-information security-related authority. (Gov. Code Sec. 11549.3(b).)

In the subdivision established by AB 670 that follows immediately thereafter, the terms "state agency" and "state entity" are both used in reference to the duties of OIS pertaining to ISAs. (Gov. Code Sec. 11549.3(c).) Here, the construct of the subdivision suggests that "state entity" is meant to be read as an all-encompassing term that covers not only state agencies, but also offices and departments. Specifically, that subdivision states that OIS may conduct, or require to be conducted, an ISA of *every state agency, department, or office*, and then in the very next paragraph states that OIS must annually require no fewer than 35 *state entities* to perform an ISA, the cost of which shall be funded by the *state agency, department, or office* being assessed. (*Compare* Gov. Code Sec. 11549.3(c)(1) to Gov. Code Sec. 11549.3(c)(2)(A).) And while the term "state entity" in that subdivision has <u>not</u> been specifically tied back to the same narrow definition in Section 11546.1 as it has been in the previous subdivision, it appears that all of this language has created much confusion as to the authority of OIS over offices in the Executive Branch, not all of whom report directly to the Governor, such that OIS seemingly cannot always, or at least in a timely fashion, perform the responsibilities with which the Legislature charges them under this statute.

This discrepancy between the intent of the Legislature and the actual statutory language is further highlighted by later legislation in the realm of cybersecurity under the Emergency Services Act, which clearly envisions CDT to have broader authority under Section 11549.3 than the "state entity" language above might suggest. The Emergency Services Act, as amended by AB 1022 (Irwin, Ch. 790, Stats. 2017), expressly states that CDT, in consultation with Cal OES and *in compliance with Section 11549.3*, above, must update the Technology Recovery Plan element of the State Administrative Manual to ensure the inclusion of cybersecurity strategy incident response standards *for each state agency* to secure its critical infrastructure controls and critical infrastructure information. (Gov. Code Sec. 8592.35(a)(1).) Under that Act, "state agency" is expressly defined to have the same meaning as in Section 11000, i.e. the broader default definition of "state agency" used throughout the Government Code.

This bill seeks to rectify cybersecurity shortcomings resulting from this inconsistency by requiring all state agencies and entities to comply with substantively similar information security polices, standards, and procedures.

5) **Non-compliance of "non-reporting" entities**: Due to the ambiguity resulting from the various uses of the terms "state agency" and "state entity" in the requirements to comply with OIS information security standards and practices and undergo mandatory ISAs, several state entities have contended that they are not, in fact, subject to these requirements. In particular, so-called "non-reporting entities," i.e. state entities that are not under the direct authority of, and thus do not report to, the Governor, have seemingly interpreted the statute to be

inapplicable to their circumstances, since they may not be included in the referenced definition of "state entities" provided by Section 11546.1. This includes "constitutional officers," i.e. those Executive Branch officers specifically provided for by the California Constitution, including the Lieutenant Governor, Attorney General, Controller, Insurance Commissioner, Secretary of State, Superintendent of Public Instruction, Treasurer, members of the State Board of Equalization, and the State Auditor. To clarify the legal validity of this interpretation, in 2018, former Asm. Obernolte requested an opinion from the Legislative Counsel addressing two related questions: 1) are the constitutional officers "state entities" for purposes of Section 11549.3(b), i.e. required compliance with OIS information security policies and standards, and; 2) is a constitutional officer subject to the ISAs described in Section 11549.3(c)(1)? In response to the first question, the Legislative Counsel opined:

> [I]n order to be a "state entity" under section 11546.1, the executive branch entity must [] be *under the direct authority* of the Governor. The constitutional officers, although a part of the executive branch, are not under the direct authority of the Governor; they are elected independently of the Governor, and have separate functions over which the Governor does not exercise direct authority. […] Accordingly, it is our opinion that the constitutional officers do not fit the definition of "state entity" in section 11546.1, and therefore are not "state entities" for purposes of section 11549.3, subdivision (b).[2]

The Legislative Counsel viewed the second question as more complex, and less certain in its proper legal interpretation. Though the opinion provided arguments both for and against constitutional officers being subject to the ISA requirements, it ultimately concluded:

> [W]e conclude that the definition of "state agency," provided for in section 11000 includes the constitutional officers. Thus, because we think a court would likely find that the definition of "state agency" provided for in section 11000 would apply to the use of that term in section 11549.3, subdivision (c)(1), it is our opinion that a constitutional officer is subject to the security assessments described in that provision.

In other words, the Legislative Counsel's analysis of the issue determined it likely to be the case that while constitutional officers (and potentially other non-reporting entities) are not obligated under current law to comply with the information security standards, policies, and practices issued by OIS, they are bound by the requirements pertaining to ISAs.

Nonetheless, this reasoning has not been tested in a court of law, and thus the ultimate interpretation of these statutes remains unresolved. Non-reporting entities have consistently interpreted the law as inapplicable to them both in terms of compliance with OIS standards, and in terms of compliance with ISA requirements. To resolve any ambiguity and ensure sufficient information security across all state entities, this bill aims to apply clear information security standards and ISA requirements to these entities.

6) **AB 3193 and the independence concerns of constitutional officers**: In 2018, Asm. Chau, along with Asms. Irwin and Obernolte, proposed AB 3193 (Chau, 2018), which sought to align the language of statute with the Legislature's apparent intent by clarifying that all state agencies under the broad definition provided by Section 11000, including constitutional

---

[2] Diane F. Boyer-Vine & Richard L. Mafrica, "State Government: Information Security - #1814902," *Legislative Counsel Bureau*, Opinion, Dec. 13, 2018.

officers and other non-reporting entities, were required to comply with security and privacy policies and incident notification requirements established by OIS, and to undergo mandatory ISAs. In short, this would have provided consistent CDT oversight across every state office, officer, department, division, bureau, board, and commission.

AB 3193 died in the Senate Governmental Organization Committee, and was opposed by several state constitutional officers, including the Secretary of State, the State Controller, the Insurance Commissioner, the State Treasurer, and the State Superintendent of Public Instruction, on the grounds that it could threaten their independence and their ability to fulfill their constitutional role as an institutional check on the power of the Governor. Those opponents argued:

> The independence of California's constitutional offices is part of the State's system of checks and balances, which mitigates the risk that an entity external to the authority of the constitutionally elected office holder, can unduly erode that independence and place burdens of responsibility, financial or otherwise, which do not align with the priorities of the elected official.

This bill aims to address these concerns by providing oversight authority for information security practices of non-reporting entities to the Legislature, a body not bound by the authority of the Governor, rather than to CDT.

7) **Reports by the State Auditor highlight critical weaknesses in the information security practices of non-reporting entities**: In July 2019, the California State Auditor published a report entitled "Gaps in Oversight Contribute to Weaknesses in the State's Information Security," which detailed findings that many non-reporting entities failed to identify concrete security standards or did not comply in full with the standards they had identified. The Auditor identified this failure to establish and comply with concrete standards, and a lack of consistent oversight, as critical factors in the continued failure of non-reporting entities to resolve high risk issues within their information security programs while the reporting entities subject to CDT oversight have showed marked improvement.

   In the interest of resolving these gaps in oversight, the Auditor's report recommended that the Legislature adopt three amendments to state law:

   - Require all nonreporting entities to adopt information security standards comparable to the information security and privacy policies prescribed by CDT.

   - Require all nonreporting entities to obtain or perform comprehensive ISAs 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.

   In January 2022, the State Auditor followed up on that report with an update entitled "State High-Risk Update – Information Security: The California Department of Technology's Inadequate Oversight Limits the State's Ability to Ensure Information Security" (Report

2021-602).[3] This report primarily focused on the shortcomings of CDT in overseeing and ensuring accountability for the compliance of reporting entities with information security and privacy standards issued by OIS. Nonetheless, the report again took specific note of the uniquely poor information security practices of non-reporting entities. According to the report:

> [W]hen we surveyed 32 nonreporting entities, we found that they also have not adequately addressed their information security. Although 29 of the 32 nonreporting entities have adopted an information security framework or standards, only four reported that they had achieved full compliance with their chosen framework or standards. […] In our previous report, we identified gaps in oversight that have contributed to nonreporting entities' information security weaknesses. [Citation.] We also noted that some non-reporting entities have an external oversight framework that requires them to assess their information security regularly. We found that nonreporting entities with external oversight were generally further along in their information security development than those without such oversight. Given the value of external oversight of information security and considering our recent survey results, the Legislature should create an oversight structure for all nonreporting entities.[4]

To achieve this, the 2022 report recommended that the Legislature take a modified form of the approach recommended in the 2019 report, as follows:

> [Amend state law to] require each nonreporting entity to adopt information security standards comparable to those required by CDT and to provide a confidential, annual status update on its compliance with its adopted information security standards to legislative leadership, including the president pro tempore of the California State Senate, the speaker of the California State Assembly, and minority leaders in both houses. It should also require each nonreporting entity to perform or obtain an audit of its information security no less frequently than every three years.[5]

Though nearly identical to the previous recommendations, this recommendation suggests that non-reporting entities certify compliance with their adopted information security standards to legislative leadership, rather than to the Assembly Committee on Privacy & Consumer Protection. The report does not comment on the relative merits of reporting to legislative leadership rather than to this Committee, but does indicate that one advantage of oversight by legislative leadership rather than CDT is the Legislature's leverage through budget authority to incentivize non-reporting entities to comply with information security requirements.[6] The critical role of legislative leadership in budget negotiations could therefore be a factor in encouraging this change. This bill seeks to implement the updated recommendation from the Auditor's report.

8) AB 809 (Irwin, 2021) sought to implement the Auditor's initial recommendations: In 2021, the author of this bill introduced AB 809, which sought to revive the objectives of AB

---

[3] Michael S. Tilden, "State High-Risk Update – Information Security: The California Department of Technology's Inadequate Oversight Limits the State's Ability to Ensure Information Security," *Auditor of the State of California*, Report 2021-602, January 2022.
[4] *Id.* at pp. 2-3.
[5] *Id.* at p. 3.
[6] *Id.* at p. 31.

3193 without infringing on the independence of non-reporting entities from the authority of the Governor and other reporting entities. First, AB 809 would have required any state agency, as broadly defined by Section 11000, that is not bound by the required standards, practices, and ISAs issued and overseen by OIS, to adhere to standards meeting certain federally-established criteria rather than to standards established by OIS, though the latter option would still have been permitted. Second, AB 809 would have required that these agencies carry out ISAs every two years, rather than at the behest of OIS. Finally, AB 809 would have required agencies subject to these provisions to annually certify to this Committee, the Assembly Committee on Privacy and Consumer Protection, that they are in compliance with all policies, standards, and procedures adopted pursuant to the bill, including corrective action plans to address any outstanding deficiencies, estimated dates of compliance, and additional resources required to cure each deficiency.

These changes seemed to effectively address many of the concerns expressed by opponents of AB 3193. By requiring compliance with internal standards consistent with federal best practices rather than OIS standards, the bill would have avoided subjecting non-reporting entities, including constitutional officers, to standards that could "unduly erode [the] independence [of the constitutional offices]" and would have avoided "burdens of responsibility…which do not align with the priorities of the elected official." Consistent with the Auditor's recommendation that all non-reporting entities "adopt information security standards comparable to SAM 5300," (i.e., the standards issued by OIS), compliance with these standards by an agency not subject to those issued by OIS would have ensured that minimum information security and privacy standards are in place across all state agencies, and that those standards were developed with the expertise to effectively safeguard public networks, without infringing on the independence of non-reporting entities.

AB 809 would also have enacted the Auditor's initial recommendation to require annual certification to this Committee that the agency is in compliance with the policies, standards, and procedures it has adopted, and to include in that certification corrective action plans addressing outstanding deficiencies, estimated dates they expect to attain compliance, and additional resources they may need to cure the deficiency. However, some concerns were raised by affected non-reporting entities that the corrective action plans submitted to this Committee may require disclosure of highly sensitive information that could, if compromised, place those entities, and the critical services for which they are responsible, at significant risk. AB 809 passed unanimously out of this Committee and the Assembly Committee on Accountability & Administrative Review before being held on suspense in the Assembly Appropriations Committee.

This bill would take a nearly identical approach to AB 809 with specific modifications to align the bill's provisions with the Auditor's updated recommendation and to address the security concerns raised by non-reporting entities.

9) **AB 2135 retains key provisions of AB 809 with minor changes to better conform with the Auditor's recommendation and address concerns of non-reporting entities**: AB 2135 is virtually identical to AB 809 with four key exceptions: 1) rather than certifying to this Committee, AB 2135 would require certification to legislative leadership, consisting of the President pro Tempore of the Senate and the Speaker of the Assembly, that the agency is in compliance with all policies, standards, and procedures adopted pursuant to the bill's provisions; 2) rather than requiring the certification to include, generally, a corrective action

plan addressing outstanding deficiencies, estimated dates of expected compliance, and additional resources needed to cure the deficiency, AB 2135 would require that the certification include a standardized accounting of information security risks and deficiencies prescribed in the SIMM known as a POAM; 3) AB 2135 would include current versions of the referenced federal standards and would clarify that policies, standards, and procedures should adhere to these current versions *and their successor publications*, if and when updated standards are released; and 4) AB 2135 clarifies that a non-reporting entity may contract with the Military Department, *or with a qualified responsible vendor*, to perform an ISA. These latter two changes are technical and clarifying in nature, and ensure that state agencies adopting the federal standards and procedures are using the most up-to-date publications, and that the authorization for non-reporting entities to contract with the Military Department for ISAs is not misinterpreted to preclude contracting with other qualified third-party vendors with the requisite expertise to adequately conduct the assessment.

The first major difference between this bill and AB 809, that certification of compliance with adopted standards shall be provided to legislative leadership rather than to this Committee, mirrors the same change in the recommendation of the State Auditor. Despite the change, the bill nonetheless retains the oversight authority of the Legislature with respect to the information security status of non-reporting entities. The information security and privacy standards issued by OIS and published in the State Administrative Manual Section 5300, et seq., require reporting entities to obtain various assessments and annually certify their compliance with those standards to OIS. Since non-reporting entities are not subject to these requirements, they are not accountable to OIS for compliance with any set of security and privacy standards, creating a critical gap in accountability for non-reporting entities with respect to their information security practices. As discussed in Comment 7, above, the Auditor's reports suggest that this lack of external oversight likely results in less rigorous assessment of information security status, and less expedient resolution of any identified shortcomings. However, the Auditor's report also recognized the independence concerns of non-reporting entities, and suggested that Legislative oversight, rather than external oversight by another executive entity, may be an appropriate solution:

> These examples demonstrate the value of establishing an oversight framework for nonreporting entities. However, several nonreporting entities have previously expressed concern that reporting to [CDT] would jeopardize their independence; therefore, the Legislature may be better positioned to oversee nonreporting entities. It could amend state law to provide a confidential mechanism for these entities to share highly sensitive information about their information security status.

To provide necessary accountability for non-reporting entities while preserving their independence from the authority of the Governor and other reporting entities, AB 2135 would require annual certification of compliance by non-reporting entities to legislative leadership, consisting of the President Pro Tempore of the Senate and the Speaker of the Assembly. This would allow the Legislature to engage as necessary with entities that are not meeting their responsibilities under the provisions of this bill, or are not satisfactorily rectifying vulnerabilities in a timely manner. Though the Auditor's report does not provide justification for the change in recipient from their previous recommendation of certifying compliance to this Committee, considering the integral role of legislative leadership in annual budget negotiations, legislative leadership may have more tangible leverage to enforce compliance relative to this Committee. The bill also provides leadership with the

authority to share the information contained therein with members of the Legislature and legislative employees at leadership's discretion, provided a chain of custody is maintained, and instructs legislative leadership to consult with the relevant state agencies on policies and procedures for transferring, receiving, possessing, or disclosing certifications to ensure confidentiality and security of the certification.

Though AB 809 contained explicit confidentiality requirements with respect to compliance certifications shared with the Legislature, several non-reporting entities nonetheless raised concerns that the inclusion of a corrective action plan addressing outstanding deficiencies, estimated dates of expected compliance, and additional resources needed to cure the deficiency, could expose critical vulnerabilities that would put the digital infrastructure of the agencies at further risk if inadvertently or haphazardly disclosed. These concerns arose, in part, from a lack of clarity concerning the level of detail required when reporting this information. According to the author:

> The content of the reports to the Legislature, including corrective action plans, have been a point of concern. Non-reporting entities do not wish to share sensitive information that can identify their vulnerabilities; however, effective oversight necessitates seeing both the bad and the good. The author has discussed previously the relatively sparse and summary nature of CDT's Plan of Action and Milestones (POAMs) as an example of what a corrective action plan would look like under the bill.

The SIMM describes a POAM as follows:

> Each state entity is responsible for establishing an Information Security Program to effectively manage risk […] including a Risk Register and Plan of Action and Milestones (POAM) process for addressing information security program deficiencies.
>
> POAMs are submitted to [OIS] to create a statewide perspective and status of a state entity's efforts to achieve full compliance. POAMs are updated throughout program maturation through compliance self-reporting, and in response to risk assessments and audit findings, incidents, and oversight reviews. The standardized format will provide Agencies/state entities with a standardized tool and provide for consistency in reporting to OIS. (SIMM Sec. 5305-B.)

The SIMM provides detailed instructions and a standardized form for completing a POAM to ensure consistency in reporting and facilitate the timely assessment of cybersecurity status. The POAM form includes requests for information including, among other things: a brief description of the nature and characteristics of the risk; a brief description of the information asset(s) that may be impacted by the risk; a brief description of any short or long-term compensating controls installed; a brief description of the high-level steps the Agency/state entity will take to address the risk; the likelihood that the threat will occur and the finding will be exploited; the impact if the finding is exploited; and general timelines for addressing the risk. Notably, all descriptions of vulnerabilities required by the POAM are high-level summaries, rather than specific details that could expose the entities to further risk.

That said, the language of AB 809 did not specify that a POAM would be sufficient to satisfy the certification requirements, leaving ambiguity as to what information the Legislature may demand. To resolve this concern, the author has prudently updated the certification specifications in AB 2135 to explicitly require that the certification "include a risk register

and plan of action and milestones pursuant to the Statewide Information Management Manual (SIMM) Section 5305-C." This, along with the maintenance of a chain of custody for any information shared beyond the Speaker and President Pro Tempore, seems likely to provide sufficient assurance of the security and confidentiality of this sensitive information.

With these updates, AB 2135 seems to strike an appropriate balance between providing essential baseline cybersecurity requirements and oversight mechanisms to better secure the information technology of state agencies, and honoring the independence and security concerns of non-reporting entities.

10) **Related legislation**: AB 1711 (Seyarto) would require a person or business operating an information system on behalf of an agency that is required to disclose a breach of that system pursuant to existing law, to also disclose the breach by conspicuously posting the requisite notice on the agency's website, if the agency maintains one.

AB 2190 (Irwin) would enact a recommendation from the State Auditor's 2022 report (*see* Comment 7) to require that CDT confidentially submit an annual statewide information security status report, including specified information, to the Chair of the Assembly Committee on Privacy & Consumer Protection no later than January 2023.

AB 2355 (Salas) would require a local educational agency (LEA), as defined, to report any cyberattack, as defined, that impacts more than 500 pupils and personnel to Cal-CSIC; AB 2355 would further require that Cal-CSIC establish a database that tracks reports of cyberattacks submitted by LEAs, and that Cal-CSIC annually report to the Governor and the relevant policy committees of the Legislature specified information concerning cyberattacks affecting LEAs.

Prior legislation: AB 809 (Irwin, 2021) *See* Comment 8.

AB 2669 (Irwin, 2020) was substantially similar to AB 809 (Irwin, 2021). AB 2669 was not heard in this Committee due to constraints on the legislative processes imposed by the COVID-19 pandemic.

AB 2813 (Irwin, Ch. 768, Stats. 2018) established, within Cal OES, Cal-CSIC, with the primary mission to reduce the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, or public and private sector computer networks.

AB 3075 (Berman, Ch. 241, Stats. 2018) created the Office of Elections Cybersecurity within the Secretary of State, tasked with the primary mission to coordinate efforts between the Secretary of State and local elections officials to reduce the likelihood and severity of cyber incidents that could interfere with security or integrity of elections.

AB 3193 (Chau, 2018) *See* Comment 6.

AB 1022 (Irwin, Ch. 790, Stats. 2017) *See* Comment 4.

AB 670 (Irwin, Ch. 518, Stats. 2015) *See* Comment 3.

AB 1172 (Chau, 2015) would have continued the existence of the California Cyber Security Task Force created by Governor Brown within the Office of Emergency Services until 2020,

to act in an advisory capacity and make policy recommendations on cybersecurity for the state, and would have created a State Director of Cyber Security position with specified duties within the Office of Emergency Services. This bill died on the Senate Inactive File.

AB 2408 (Smyth, Ch. 404, Stats. 2010) *See* Comment 3.

11) **Double-referral**: This bill has been double-referred to the Committee on Accountability and Administrative Review.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

Analysis Prepared by: Landon Klein / P. & C.P. / (916) 319-2200