Date of Hearing: April 8, 2021

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 809 (Irwin) – As Amended March 25, 2021

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. 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 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 the Assembly Committee on Privacy and Consumer Protection that the agency is in compliance with all policies, standards, and procedures adopted pursuant to the bill, including corrective action plans to address any outstanding deficiencies, the estimated dates of compliance, and any additional resources the agency requires in order to cure each deficiency.

6) Specify that, notwithstanding any other law, the certification made pursuant to 5), above, shall not be disclosed, except that the information and records may be shared with the members of the Legislature and legislative employees, at the discretion of the chairperson of the Committee.

EXISTING LAW:

1) Establishes, within the Government Operations Agency, the Department of Technology, 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 Department of Technology, 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 Section 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.)

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:

> In 2019 the State Auditor published a report entitled "Gaps in Oversight Contribute to Weaknesses in the State's Information Security" which uncovered startling findings that many state agencies, termed "non-reporting entities" for their independence from reporting to the Governor, had either failed to identify information security standards to follow, or were only partially compliant with the standards they had identified.
>
> The Auditor identified that failure to formally adopt information security standards and a lack of consistent oversight of these agencies as a key reason behind their continued failure to resolve high risk issues within their information security programs, in contrast to the marked improvement of "reporting entities" who have improved under the leadership of the California Department of Technology (CDT).
>
> 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. […]
>
> AB 809 requires all state agencies, but not those who report directly to the Governor, to adopt and comply with NIST and FIPS cybersecurity standards and reporting requirements. It provides voluntary authority for these agencies to adopt SAM 5300 standards which are followed by the remainder of state government. The bill requires these state agencies to conduct ISAs every two years, and authorizes them to contract with the Military Department to conduct them. Finally the bill requires these state agencies to report on their compliance, including corrective action plans to this Committee.

3) State investments in cybersecurity: As society's reliance on technology grows, so too do the vulnerabilities to and costs associated with cybercrime. The Federal Bureau of Investigation's Internet Crime Complaint Center (FBI IC3) reported over two million complaints of internet crime over the past five years, totaling over $13 billion dollars in resulting losses. The number of reported internet crimes has increased every year since 2016, as have the associated costs, and the margin by which these rates increase year-over-year continues to grow. Between 2019 and 2020 alone, the number of complaints received by the FBI IC3 increased by nearly 70%, from 467,361 in 2019 to 791,790 in 2020, likely as a result of unprecedented demand for virtual technologies resulting from the COVID-19 pandemic. According to the FBI IC3's 2020 report, California leads the nation in both the number of complaints relating to internet crime, and in the estimated costs experienced by the victims.[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. In 2015, Executive Order B-34-15 required the Office of Emergency Services (Cal OES) to establish and lead the California Cybersecurity Integration Center (Cal-CSIC), with the primary mission to reduce the likelihood and severity of cyber incidents

---

[1] Internet Crime Complaint Center, "Internet Crime Report 2020," *Federal Bureau of Investigation*, March 2021, https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics, [as of Mar. 28, 2021].

that could damage California's economy, critical infrastructure, or public and private sector computer networks. The existence of Cal-CSIC was codified three years later by AB 2813 (Irwin, Ch. 768, Stats. 2018). In 2018, the Legislature passed AB 3075 (Berman, Ch. 241, Stats. 2018) which 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 the security or integrity of elections. The Budget Act of 2020 (AB 89, Ting, Ch. 7, Stats. 2020) also made substantial investments in cybersecurity, including allocating $11.1 million to various departments to enhance the cybersecurity of the State's critical infrastructure, and $2.9 million to protect patient health records by strengthening cybersecurity throughout the State's public health 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 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 the Office of Emergency Services (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 809 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), 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.

Committee staff further notes that even the reference to "state entity" for purposes of defining which offices must comply with OIS policies and procedures is rather confusing. Whereas the debate has been centered mostly on whether or not executive branch offices outside the direct authority of the Governor should follow the information security policies and procedures set by OIS, there is an even more narrow interpretation that is wholly illogical and untenable as a result of the drafting of these statutes. Namely, because state entities are those departments, boards, bureaus, commissions, councils, and offices *that are not defined as a "state agency,"* and state agency means the various umbrella agencies such as the Transportation Agency, Business, Consumer Services, and Housing Agency, Natural Resources Agency, California Health and Human Services Agency, California Environmental Protection Agency, etc., there is a plausible reading of this statute that suggests even those agencies (which are under the Governor's direct authority) do not have to comply with OIS policies and procedures or file reports as required by OIS. While this particular delineation of agencies and entities may make sense in the context of differentiating *state agencies* that must have chief information officers that are technically considered "Agency Information Officers," from *state entities* that must have "chief information officers" that report to agency information officers, it does not make sense as a matter of public policy in the context of ensuring the state has strong and more or less uniform information security policies and procedures across state government.

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) **"Gaps in Oversight contribute to weaknesses in the State's Information Security"**: 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. The report's summary described the situation as follows:

> Gaps in oversight weaken the State's efforts to keep its information secure. Although we previously found that [CDT] has made progress in its oversight since our initial 2013 assessment, and the state entities subject to its oversight have increased their compliance with established standards, state entities that do not fall under the purview of [CDT] need to do more to safeguard the information they collect, maintain, and store. State law generally requires state entities within the executive branch under the Governor's direct authority (reporting entities) to comply with information security and privacy policies that [CDT] prescribes. However, state law does not apply [CDT's] policies and procedures to entities that fall outside of that authority (nonreporting entities). […]

---

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

> The nonreporting entities we surveyed may be unaware of additional information security weaknesses because many of them relied upon information security assessments that were limited in scope. […] Although nonreporting entities are not subject to [CDT's] policies and procedures, some are subject to an oversight framework that requires them to assess their information security regularly. This was the case for three of the four entities that had fully assessed their selected standards, leading us to conclude that external oversight improves a state entity's information security status. At the same time, nonreporting entities without external oversight that fail to routinely assess their level of compliance with adopted security standards and then fail to address identified deficiencies are placing some of the State's sensitive data at risk of unauthorized use, disclosure, or disruption.[3]

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.

AB 809 would actualize these recommendations from the Auditor's report.

7) **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 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:

---

[3] Elaine M. Howle, "Gaps in Oversight Contribute to Weaknesses in the State's Information Security: High Risk Update – Information Security," *Auditor of the State of California*, Report 2018-611, July 2019.

> 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.

As discussed more fully below, AB 809 seeks to revive the objectives of AB 3193, i.e. ensuring sufficient security and privacy standards and oversight across state agencies, without infringing on the independence of non-reporting entities from the authority of the Governor and other reporting entities.

8) **AB 809 would use federal standards and Legislative oversight to avoid potential intrusions on the independence of constitutional officers**: AB 809 is a reintroduction of last year's AB 2669 (Irwin, 2020), which did not receive a hearing in this Committee due to constraints on the legislative process imposed by the COVID-19 pandemic. AB 809 differs from AB 3193 in three key ways. The first is that the bill requires any state agencies, as broadly defined by Section 11000, that are 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 is still permitted. The second is that the bill requires that these agencies carry out ISAs every two years, rather than at the behest of OIS. Finally, the bill requires 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 seem to effectively address the concerns expressed by opponents of AB 3193. By requiring compliance with internal standards consistent with federal best practices rather than OIS standards, yet permitting the latter, the bill would avoid subjecting non-reporting entities, including constitutional officers, to standards that could "unduly erode [the] independence [of the constitutional offices]" and would avoid "burdens of responsibility…which do not align with the priorities of the elected official." OIS could not, for instance, impose standards that they know will be particularly onerous for the Department of Justice in order to extort that Department on behalf of the Governor's interests. Instead, should a non-reporting entity elect to adopt and implement their own information security and privacy policies, standards, and procedures rather than those issued by OIS, those policies, standards, and procedures would be required to adhere to federal standards set forth by all of the following: the National Institute of Standards and Technology (NIST) "Security and Privacy Controls for Federal Information Systems and Organizations" (Special Publication 800-53, Revision 4); Federal Information Processing Standards (FIPS) 199 "Standards for Security Categorization of Federal Information and Information Systems," and; FIPS 200 "Minimum Security Requirements for Federal Information and Information Systems."

   Together, these standards promulgated by NIST are intended to be both comprehensive and broadly applicable. For instance, the NIST "Security and Privacy Controls," supra, are described as providing "a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other

organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks," and indicates the controls therein to be "flexible and customizable [to] address diverse requirements derived from mission and business needs, laws, executive orders, directives, regulations, policies, standards, and guidelines." Similarly, FIPS 199 describes its purpose as "to provide a standard for categorizing federal information and information systems according to an agency's level of concern for confidentiality, integrity, and availability and the potential impact on agency assets and operations should their information and information systems be compromised through unauthorized access, use, disclosure, disruption, modification, or destruction." Though these standards are formulated primarily for use by federal agencies, they are intended to be generally applicable across diverse agencies and organizations, and nonetheless provide a thoroughly vetted, up-to-date framework designed to manage the types of information and information systems that agencies, whether federal or state, are expected to encounter. 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 ensure that minimum information security and privacy standards are in place across all state agencies, and that those standards are developed with the expertise to effectively safeguard public networks, without infringing on the independence of non-reporting entities.

Additionally, by requiring regular ISAs every two years, rather than at the behest of OIS, OIS cannot use these assessments to harass or impede the operations of a constitutional office who may be, at any given time, serving as a check to the Governor's authority. This requirement would therefore allow for independent evaluation of the information security standing of all agencies either through ISAs requested by OIS or through ISAs required by this periodic schedule, consistent with the Auditor's recommendation that non-reporting entities undergo ISAs no less frequently than every three years.

9) **Certifying information security standard compliance to this Committee**: This bill would enact the Auditor's 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. 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. This lack of external oversight likely results in less rigorous assessment of information security status, and less expedient resolution of any identified shortcomings. As the Auditor's report notes:

> Most of the nonreporting entities we reviewed asserted that they did not have an external oversight framework that would require them to assess their information security regularly. However, we noted that those few nonreporting entities that were subject to such a requirement typically assessed more of their selected information security standards than those that had no such requirement. […] Without the accountability that

> external oversight provides, nonreporting entities may be less likely to resolve information security issues in a timely manner.

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 809 would require annual certification of compliance by non-reporting entities to this Committee, including corrective action plans for resolving any issues and timelines and resources necessary for resolution. This would allow this Committee 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.

Some concerns have been 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. It should be noted that the Legislature, like agencies in the Executive Branch, is accustomed to handling sensitive information and maintains standards and procedures for mitigating risks of unauthorized access to confidential materials. Nonetheless, to further secure these certifications against unauthorized access and associated risks, the author has prudently amended the bill to specify that "[n]otwithstanding any other law, the certification made to the committee shall be kept confidential and shall not be disclosed, except that the information and records may be shared with the members of the Legislature and legislative employees, at the discretion of the chairperson of the committee." This would allow the chairperson the capacity to share these certifications with the parties necessary to ensure adequate accountability, while minimizing their dissemination to prevent inadvertent disclosure or unauthorized access.

10) **Related legislation**: AB 581 (Irwin) would require all state agencies, no later than July 1, 2022, to review and implement NIST guidelines for reporting and resolution of security vulnerabilities issued pursuant to the federal Internet of Things Cybersecurity Improvement Act of 2020 (PL 116-207), and would provide that agencies under the direct authority of the Governor shall satisfy this requirement by implementing standards and procedures published by the chief of OIS based on the NIST guidelines.

AB 1352 (Chau) would authorize the Military Department to perform an ISA of a local educational agency or schoolsite at the request and expense of the local educational agency.

Prior legislation: AB 89 (Ting, Ch. 7, Stats. 2020) *See* Comment 3.

AB 2669 (Irwin, 2020) *See* Comment 8.

AB 2813 (Irwin, Ch. 768, Stats. 2018) *See* Comment 3.

AB 3075 (Berman, Ch. 241, Stats. 2018) *See* Comment 3.

AB 3193 (Chau, 2018) *See* Comment 7.

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) 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