Date of Hearing: April 19, 2022

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
AB 2190 (Irwin) – As Introduced February 15, 2022

SUBJECT: Office of Information Security: annual statewide information security status report

SUMMARY: This bill would require that the chief of the Office of Information Security (OIS) submit an annual statewide information security status report including specified information to the Assembly Committee on Privacy and Consumer Protection (this Committee) beginning no later than January 2023. Specifically, **this bill would**:

1) Require the chief of OIS to submit an annual statewide information security status report to this Committee.

2) Specify that the report pursuant to 1), above, shall include the maturity metric scores it has calculated for each state agency or state entity, as defined, and the results of the National Cyber Security Review for each state agency or state entity, as conducted by the United States Department of Homeland Security (DHS) and the Multi-State Information Sharing and Analysis Center.

3) Require that the chief of OIS submit the first report no later than January 2023; and specify that this report shall include the Department of Technology's (CDT's) plan for assisting state agencies and state entities in improving their information security.

4) Provide that, notwithstanding any law, the status report and any information or records included with the status report shall be confidential and shall not be disclosed, except to members of the Legislature and legislative employees, at the discretion of the chairperson of this Committee.

5) Make legislative findings and declarations demonstrating the alleged state interest protected by the bill's limitation imposed on the public's right of access to the meetings of public bodies or the writings of public officials and agencies, and the need for protecting that interest.

EXISTING LAW:

1) Establishes, within the Government Operations Agency, 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, 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 independent security assessment (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 improve the Legislature's oversight of CDT's role in protecting the cybersecurity of state agencies under the Governor's direct authority by requiring OIS to submit annual reports to this Committee detailing the maturity of the cybersecurity policies and practices of state agencies as quantified by both state and federal assessments.

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

> The [State] Auditor's report details a stagnation and slight decline in the cybersecurity posture of state agencies over their multi-year review of CDT's OIS security oversight cycles, which focus on independent security assessments and audit programs. The Auditor also noted in its review of CDT's briefings of the Chairs of the [Assembly]

Select Committee on Cybersecurity and [the Assembly Committee on Privacy & Consumer Protection]:

> We reviewed CDT's presentations and found that it shared high-level information with the Legislature about its compliance audits []. However, CDT generally did not share more detailed information – such as the results of the nationwide review and the maturity metric scores it has calculated – that would have provided the Legislature with a more comprehensive picture of reporting entities' information security statuses. In the absence of complete information, the Legislature lacks perspective on the significant weaknesses that exist in the State's information security and thus cannot take appropriate steps to hold CDT and reporting entities accountable.

[…] To avoid the Legislature providing incomplete oversight, and to enable the Legislature to better support the Executive branch's performance on their own maturity metric scores, a more formalized and robust reporting system needs to be established. This bill enacts the Auditor's recommendation in their report 2021-602 [which requires] that CDT confidentially submit an annual statewide information security status report, including the maturity metric scores it has calculated and the results of the nationwide review, to the appropriate legislative committees [including] CDT's plan for assisting reporting entities in improving their information security.

3) **CDT, OIS, and oversight of state cybersecurity**: CDT is tasked, among other things, with providing technology direction to agencies and departments to ensure the integration of statewide technology initiatives, compliance with IT policies and standards, and the effective management of IT services. (Gov. Code Sec. 11545(b).) Within CDT, OIS was established to "ensure the confidentiality, integrity, and availability of state systems and applications, and to promote and protect privacy as part of the development and operations of state systems and applications to ensure the trust of residents of this state." (Gov. Code Sec. 11549(a).) The duties of OIS under this mandate explicitly include providing direction for information security and privacy to state government agencies, departments, and offices (Gov. Code Sec. 11549(c)).

   In 2010, this 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 under the direct authority of the Governor,[*] 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).)

   In 2015, this 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

---

[*] Whether state agencies that are *not* under the direct authority of the Governor must comply with the standards, policies, and procedures issued by OIS under existing law is a topic of dispute; for further exploration of this controversy, see this Committee's analysis of AB 809 (Irwin, 2021).

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 California Cybersecurity Integration Center (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)(2)(B).)

According to the CND unit's ISA Notification Guide:

> The ISA is a technical assessment of a state entity's network and selected web applications, to identify security vulnerabilities and provide concrete, implementable actions to reduce the possibility of damaging security breaches. The ISA utilizes a series of technical controls based on [the National Institute of Standards & Technology (NIST)] Special Publication 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations" and the State Administrative Manual (SAM), Chapter 5300 "Information Security" as selected by [OIS]. […] ISAs are performed either by [the CND unit] or by a 3rd party upon the approval of OIS.

The CND unit's ISA Preparedness Guide v4.1 adds:

> The goal of the assessment is to provide an external party review of the entity's current cybersecurity state and to provide recommendations for improvement where appropriate. The assessment criteria analyze a series of foundational cybersecurity technical controls, designated by the [OIS].

AB 670 also permitted OIS to conduct, or require to be conducted, an audit of information security to ensure compliance with the information security program established by OIS. These audits are distinguished from ISAs in that the audits assess the entity's adherence to the state's information security and privacy policies, while the ISAs evaluate the actual implementation, configuration, and practices of the entity's information security program.

AB 670 additionally required OIS, in consultation with Cal OES, to determine criteria and rank state entities based on an information security index analyzing the relative amount of sensitive information the agency maintains, as well as the agency's self-certification of compliance and indicators of noncompliance with information security management provisions. (Gov. Code Sec. 11549.3(c)(2).) Based on those rankings, CDT prioritized 52 high-risk entities to participate in a four-year oversight life cycle to independently verify the status of their information security, including an initial compliance audit, a follow-up review, and two ISAs. The remaining lower-risk entities were selected to instead participate in a two-year oversight cycle including one ISA and a self-assessment of their information security development.

To standardize evaluation of these entities, CDT established the California Cybersecurity Maturity Metrics, which combine the results of the compliance audits and ISAs into a single score summarizing the entity's information security development. The maturity metrics assess the performance of the entity across five information security functions, based on the Cybersecurity Framework developed by the National Institute of Standards & Technology

(NIST). The five core functions (identify, protect, detect, respond, and recover) correspond to the entity's progress in achieving each of the following, respectively:

- Identify: establishing and maintaining an inventory of the information assets that support critical business functions and identify related cybersecurity risks.

- Protect: implementing appropriate safeguards to ensure protection of the entity's information assets.

- Detect: implementing appropriate mechanisms to identify the occurrence of cybersecurity incidents.

- Respond: developing techniques to contain the impacts of cybersecurity events.

- Recover: implementing the appropriate processes to restore capabilities and services impaired because of cybersecurity events.

Maturity metrics weight those criteria and are calculated on a scale of 0-4, with a score of 0-2 indicating the entity is "still working to develop the foundational components of their information security program or have developed them, whereas entities that score a value of 3-4 have already implemented their procedures and have demonstrated varying levels of effectiveness."[1] Each four-year oversight life cycle is intended to yield a maturity metric score.

In addition to ISAs and compliance audits, CDT also requires state entities under the direct authority of the Governor to participate in various self-reporting mechanisms relating to their information security. The self-assessments required by CDT include annual completion of the federal Nationwide Cybersecurity Review (NCSR), completion of which is a condition for receiving security grant funding from DHS. According to the NCSR's FAQ document:

> The Nationwide Cybersecurity Review (NCSR) is a no-cost, anonymous annual self-assessment, designed to measure gaps and capabilities of state, local, tribal and territorial governments' [(SLTT)] cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). The NCSR is sponsored by the Department of Homeland Security (DHS) and the Multi-State Information Sharing and Analysis Center (MS-ISAC).
>
> The NCSR question set was built upon the NIST CSF Core, with some minor alterations. […] Each of the five functions is subdivided into a total of 23 categories and then further into 108 sub-categories. The NCSR leverages the 108 sub-categories as the questions for the assessment. For assessment purposes, the sub-categories provide enough details for organizations to identify actionable steps to improve their cybersecurity maturity and the ability to utilize pre-existing cross-references to best practices, standards, and requirements. Using the results of the NCSR, DHS delivers a bi-yearly anonymous

[1] 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.

summary report to Congress, providing a broad picture of cybersecurity maturity across the SLTT communities. […]

The NCSR is different [from other audits, surveys, assessments, reviews, etc.] in several key ways that are beneficial to the SLTT community. It is designed to measure the gaps and capabilities of cybersecurity programs, while most other audits are designed to determine compliance or adherence to a specific set of requirements. When completed on an annual basis, the NCSR allows participants to measure changes in their cybersecurity program over time.[2]

This bill would leverage these metrics to improve the Legislature's capacity to oversee state cybersecurity by requiring the chief of OIS to provide an annual report to this Committee on the state's information security status, including the maturity metric scores it has calculated for each state entity and the results of the NCSR for each state entity.

4) **State Auditor's Report 2021-602**: In January 2022, the California State Auditor published a report 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 state entities with information security and privacy standards issued by OIS. According to the report:

Although one of CDT's key roles is to oversee information security development for the State's 108 reporting entities, it has yet to fully assess the overall status of the State's information security. […] [B]ecause CDT has been slow to complete the compliance audits, it had calculated only 18 of the 39 maturity metric scores it should have determined by the conclusion of the third year of the oversight life cycle in June 2021. Despite being aware of shortcomings with its approach, CDT has failed to take proactive steps to expand its capacity to perform the compliance audits, such as hiring more auditors or repurposing existing staff. Moreover, even though CDT requires reporting entities to complete self-assessments of their information security development each year, it has not used this information to inform the overall status of the State's information security.

In fact, when we evaluated reporting entities' maturity metrics and self-reported information, we found that many entities' information security is below standards. We also found little to suggest improvement over the last several years. Moreover, because CDT generally provides information on only certain aspects of the State's information security in its reports to the Legislature, the Legislature does not have a complete picture of the deficiencies in the reporting entities' information security status.

The reporting entities' lack of progress in developing their own information security may be in part because CDT has failed to take critical steps to help them improve. For example, it did not adequately follow up with 18 of the 108 reporting entities whose

---

[2] Nationwide Cybersecurity Review, "Frequently Asked Questions, " *Center for Internet Security, Multi-State Information Sharing & Analysis Center*, https://www.cisecurity.org/-/jssmedia/Project/cisecurity/cisecurity/data/media/files/uploads/2021/09/NCSR-2021-FAQs.pdf [as of Apr. 14 2022].

[3] *Supra*, fn. 1.

> directors have not submitted required certifications indicating that they were fully aware of their entities' information security statuses, were aware of any identified risks, and recognized that all deficiencies had to be addressed. CDT also failed to hold reporting entities accountable for completing the required self-assessments for only 172 of their 3,300 critical IT systems. Consequently, the reporting entities' updates to CDT on their progress toward remediating any known weaknesses are incomplete.[4]

In order to resolve these critical insufficiencies of CDT's oversight of state cybersecurity, the Auditor recommended that the Legislature amend state law to, among other things, do the following:

> Require that CDT confidentially submit an annual statewide information security status report, including maturity metric scores and self-reported information, to the appropriate legislative committees no later than December 2022. This status report should include CDT's plan for assisting reporting entities in improving their information security.[5]

This bill seeks to enact this recommendation from the State Auditor. Substantively, this bill is nearly identical to the Auditor's recommendation, except that, in order to avoid the need for "urgency" legislation, the bill delays the initial report from OIS one month from the recommendation, until no later than January 2023. The bill also identifies this Committee (i.e. the Assembly Committee on Privacy & Consumer Protection) as "the appropriate legislative committee[]", and specifies the NCSR as the "self-reported information" accompanying the maturity metric scores.

Consistent with the Auditor's assessment, the provisions of this bill seem likely to improve the Legislatures capacity to oversee both the cybersecurity of state agencies, and the performance of CDT in meeting its objectives toward assessing the overall status of the state's information security. Because this Committee's jurisdiction includes oversight of CDT, receipt of these reports is consistent with this Committee's function, and additional information on the state's cybersecurity development has the potential to inform policy to better protect the systems and information critical to state operations.

5) Potential clarifications: Though this bill seems to provide the Legislature with information that will render it better equipped to oversee, assess, and improve the state's cybersecurity, some provisions of the bill may benefit from additional clarification**.**

Notably, the bill specifies that the annual statewide information security status report shall include the results of the NCSR and the maturity metric scores it has calculated "for each state agency or state entity," which, "as those terms are defined in Section 11546.1," refer to both state agencies under the direct authority of the Governor (i.e. "state entities") and state agencies not under the direct authority of the Governor, and thus arguably not required to comply with the standards, policies, and procedures of OIS (i.e. "state agencies"). However, because the bill requires reporting related to "each state agency *or* state entity," these provisions could arguably be interpreted to require inclusion of information only relating to state agencies, *or* information only relating to state entities, to be included in the report. This would mean that while the Legislature may ultimately receive information about both state

---

[4] *Id.* at pp. 1-2.
[5] *Id.* at p. 3.

agencies *and* state entities, information about both types of agencies would not be included in the same report. It is unlikely that this is the author's intent. To resolve this ambiguity, as the bill moves through the legislative process, the author may wish to consider referring to "each state agency *and* state entity" in paragraphs (1) and (2) of subdivision (a) in Section 11549.4.1 of the bill.

Additionally, the bill requires reporting of the maturity metric scores "it has calculated for each state agency or state entity", presumably referring to OIS, but also requires "the results of the National Cyber Security Review for each state agency or state entity". Because "state agencies" are arguably not required to comply with the information security and privacy standards, policies, and procedures issued by OIS, state agencies may not be required to complete the NCSR annually, if at all (though failing to complete the NCSR would disqualify them for DHS security grant funding). Since the bill requires only the maturity metric scores OIS *has calculated* for each "state agency," this would seem to limit the required reporting on state agencies to those that have volunteered to undergo assessment by OIS. However, the bill does not provide the same limitation for the results of the NCSR, instead requiring the NCSR results for "each state agency or state entity." This provision could be interpreted to require reporting by OIS on the NCSR results for *all* state agencies, including those who do not voluntarily subject themselves to OIS oversight. OIS is unlikely to have access to this information, and therefore would not be capable of complying. To avoid confusion with respect to this requirement, as the bill moves through the legislative process, the author may wish to consider clarifying that the report is only required to include NCSR results for state agencies to the extent they are made available to OIS.

Finally, in the bill's provision specifying the date by which the chief must submit the first report, the bill also includes a requirement that "*This* status report shall include the Department of Technology's plan for assisting state agencies and state entities in improving their information security." Though not entirely clear, this provision seems to imply that information relating to CDT's plan for assisting state agencies and entities in improving their information security must only be included in the *first* report, rather than in each annual report. Arguably, information detailing CDT's intended actions to improve the information security of state agencies would be valuable to the Legislature on an annual basis, which may have been the author's intent, and would be consistent with the Auditor's recommendation. Accordingly, as the bill moves through the legislative process, the author may wish to consider moving this reporting requirement from subdivision (b) to a new paragraph in subdivision (a) as a third requirement for the annual report.

While additional clarity may be beneficial to avoid misinterpretations of the author's intent, this bill nonetheless seems likely to better equip the Legislature to respond to the information security needs of the state.

6) **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 2135 (Irwin) would enact a recommendation from the State Auditor's 2022 report requiring 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 an ISA every two years.

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) was substantially similar to AB 2135 (Irwin, 2022). This bill died in the Assembly Committee on Appropriations.

AB 2669 (Irwin, 2020) was substantially similar to AB 2135 (Irwin, 2022). 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) would have required state agencies that do not fall under the direct authority of the Governor to comply with the information security and privacy standards, policies, and procedures issued by OIS. This bill died in the Senate Committee on Governmental Organization.

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.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

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