Date of Hearing: April 23, 2024

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 2777 (Calderon) – As Amended March 19, 2024

AS PROPOSED TO BE AMENDED

SUBJECT: Department of Technology: state agencies: California Cybersecurity Maturity Metric

SYNOPSIS

California state government maintains a vast wealth of personal information related to its 39 million residents. The potential value of this information makes California a ripe target for cybersecurity attacks. The Department of Technology (CDT), and especially the Office of Information Security (OIS) within CDT, are responsible for ensuring the confidentiality, integrity, and availability of state systems and applications, especially as they relate to cybersecurity.

A series of audits conducted by the California State Auditor have revealed that CDT is not adequately hardening California against, nor sufficiently monitoring for, cybersecurity threats. CDT utilizes what it calls a "cybersecurity maturity metric" to calculate the relative vulnerability of various state agencies, offices, and departments (hereafter referred to as "reporting entities"). The calculation of this metric requires a lengthy compliance audit, and as a result, CDT is unable to regularly apply the metric to all reporting entities.

This bill would require CDT to adjust its cybersecurity maturity metric such that it could be calculated for all reporting entities every three years. Committee amendments rework this bill to instead require the development of a new metric, the Baseline Information Security Score (BISS), which would take advantage of readily-available information and allow CDT to quickly estimate the security status of all reporting entities. Entities found to be especially vulnerable or out of compliance could then be targeted for more resource-intensive compliance audits. The 2023 State Auditor's report on CDT revealed that CDT is already working to develop this metric.

This bill is author-sponsored and has no support or opposition.

SUMMARY: Requires CDT to update its Cybersecurity Maturity Metrics such that they can be conducted every three years for each reporting entity in California. Specifically, **this bill**:

1) Requires the Department of Technology to make changes to the California Cybersecurity Maturity Metric, including the Maturity Metric Score criteria, in order to:

   a) Improve reliability, efficiency, and timeliness of reporting.

   b) Achieve a Maturity metric Score for all reporting entities every three years.

2) Defines "California Cybersecurity Maturity Metric" to mean the Statewide Information Management Manual Section 5300-C, or any successor Statewide Information Management Manual section that describes a metric that objectively measures the effective implementation of cybersecurity policies, standards, and procedures by every state agency.

3) Defines "Maturity Metric Score" to mean the Statewide Information Management Manual Section 5300-C, or any successor Statewide Information Management Manual section that describes a single score a state agency received following the completion of the calculation that reflects an agency's information security status.

4) Requires a Maturity Metric Score to be comprised of information from the two most recent independent security assessments performed on a reporting entity.

EXISTING LAW:

1) Establishes CDT in the Government Operations Agency. (Gov. Code § 11545.)

    a) Requires the Director of Technology to produce an annual information technology performance report that describes, among other things, the state's progress towards enhancing the security, reliability, and quality of its information technology networks, services, and systems.

    b) Requires CDT to establish procedures and policies required to improve the performance of the state's information technology program.

    c) Requires reporting entities to take all necessary steps to achieve the targets set forth by CDT, and requires them to report their progress to the department on a quarterly basis.

2) Requires reporting entities to submit annual summaries of their actual and projected information security costs for the preceding and current fiscal year, including federal grant funds for information security purposes. (Gov. Code § 11546.2.)

3) Establishes the Office of Information Security (OIS) in CDT. (Gov. Code § 11549.)

    a) Describes the purpose of the OIS to be "ensuring the confidentiality, integrity, and availability of state systems and applications..."

    b) Describes the duty of the OIS to be to "provide direction for information security and privacy for state government agencies, departments, and offices."

4) Requires the Chief of OIS to establish an information security program that is tasked with, among other things, coordinating the activities of state agency information security officers for the purposes of integrating statewide security initiatives and ensuring compliance with information security and privacy policies and standards. (Gov. Code § 11549.3.)

    a) Requires OIS to conduct, or require to be conducted, independent security assessments of at least 35 reporting entities each year, the cost of which is to be funded by the entities being assessed.

    b) Requires OIS to determine criteria and rank state entities based on an information security risk index.

    c) Permits OIS to conduct or require to be conducted an audit of information security to ensure program compliance.

d) Requires many state entities to implement the policies and procedures issued by the office, including complying with filing requirements and incident notification by providing timely information and reports as required by the office.

e) Requires state entities not covered by (d) to annually certify to the office that the entity is in compliance with relevant policies, standards, and procedures. Requires the certification to include a plan of action and milestones.

FISCAL EFFECT: As currently in print, this bill is keyed fiscal.

COMMENTS:

1) **The importance of cybersecurity.** According to the California State Auditor, information security measures are critical to safeguarding the State's data processing capabilities, information technology (IT) infrastructure, and data, all of which are essential public resources.[1] Without adequate information security, cyberattacks such as phishing and malware intrusions can result in the disclosure of confidential information or the shutdown of critical information systems.

Effective cybersecurity protects organizations against data breaches, helping to preserve the integrity, confidentiality, and availability of information. The downsides of inadequate cybersecurity can be severe, especially when the systems in question contain the personal information of millions of people. Data breaches can have devastating consequences ranging from identity theft to financial fraud to extortion.

Organizations that suffer from cybersecurity failures face not only immediate financial losses due to theft, but also long-term reputational damage. A breach can erode public trust, leading to a loss of partners and participants. Cybersecurity is particularly critical for government entities, especially in a significant and densely populated state like California, where state government holds the personal information of millions of its residents. From tax records and social security details to health information and immigration status, the state's databases are treasure troves of sensitive data. Protecting these data not only safeguards the privacy of individuals, but also helps maintain trust in government.

2) **The Department of Technology.** CDT is, in its own words, "tasked with securing statewide information assets by providing oversight and infrastructure for many state departments and [serving] as the custodian of information for mission-critical and essential business applications."[2] Despite this charge, CDT was recently designated a high-risk state agency by the California State Auditor.[3] In a January 2022 audit of CDT, the State Auditor found that CDT had yet to establish an overall statewide information security status for the State's 108 reporting entities:

> CDT relies on compliance audits and technical security assessments to summarize each reporting entity's information security development into a single score, called a maturity

---

[1] Michael Tilden, "The California Department of Technology's Inadequate Oversight Limits the State's Ability to Ensure Information Security," *California State Auditor*, Jan. 18, 2022, https://www.auditor.ca.gov/reports/2021-602/index.html
[2] California Department of Technology, https://cdt.ca.gov/about/
[3] Grant Parks, "The California State Auditor's Updated Assessment of Issues and Agencies That Pose a High Risk to the State," *California State Auditor*, Aug. 24, 2023, https://www.auditor.ca.gov/reports/2023-601/index.html

> metric. However, because CDT was slow to complete compliance audits, it only calculated 18 of the 39 maturity metric scores it should have determined by June 2021. Despite being aware of shortcomings with its approach, CDT failed to expand its capacity to perform compliance audits.
>
> Moreover, even though CDT requires reporting entities to complete various self-assessments of their information security each year, it does not use this information to inform the statewide security status. Nonetheless, the information CDT does have shows that reporting entities continue to perform below recommended standards, and have not improved over the last several years. However, CDT has not taken critical steps to help reporting entities improve, such as holding them accountable for identifying potential risks to their critical information systems.[4]

The State Auditor performed a follow-up audit in March 2023, and found that the issues it had flagged in its 2022 report had not been addressed:

> CDT has not ensured that the State's IT systems are adequately protected from cyberattacks that can compromise individuals' identities, shut down critical government functions, and cost the State millions of dollars to remedy. For example, CDT has stated that to improve the State's information security programs, it must be able to effectively determine the status of information security across the State as a whole and within each state agency individually. However, it has yet to determine the effectiveness of the State's information security programs. Further, in those instances when it has assessed state agencies' information security, those agencies' security statuses have tended to decline subsequently rather than improve. Moreover, CDT has not taken adequate steps to educate state agencies on the cybersecurity threat monitoring service that it provides at no cost . . . Over the past 10 years, our multiple audits of CDT have identified the same or similar problems. Nevertheless, CDT has continued to struggle to demonstrate critical aspects of leadership, such as ensuring accountability, setting priorities, demonstrating urgency, and maintaining independence. [5]

If CDT cannot accurately assess the cybersecurity status of California's reporting entities, it cannot effectively intervene when these entities fall out of compliance, or harden California against cybersecurity threats. The longer an undetected vulnerability remains unaddressed, the greater the risk to Californians' privacy and security. How can these issues be resolved? The core of CDT's cybersecurity strategy lies with its "cybersecurity maturity metrics" – however, while these metrics are informative, the in-depth audits they require make them slow and clunky. It is not feasible for CDT to calculate a maturity metric score for each reporting entity every three years.

3) **Author's statement.** According to the author:

> There have been several state agency and department cybersecurity breaches recently, exposing Californians to identity theft, financial fraud, and delays in access to essential state services. Assembly Bill 2777 would require the California Department of Technology to

---

[4] Tilden, "The California Department of Technology's Inadequate Oversight Limits the State's Ability to Ensure Information Security," *supra.*
[5] Grant Parks, "Weaknesses in Strategic Planning, Information Security, and Project Oversight Limit the State's Management of Information Technology," *California State Auditor, Apr. 20, 2023,* https://www.auditor.ca.gov/reports/2022-114/index.html

> revise its existing Cybersecurity Maturity Metrics to improve the reliability, efficiency, and timeliness when assessing the state entities' IT systems. This bill requires the department to make these revisions with a goal of completing these assessments every three years. We have a responsibility to ensure that the personal information of our constituents is kept safe and this bill advances state efforts to meet this duty.

4) **What this bill would do.** This bill would require CDT to update its cybersecurity maturity metric such that a score could be calculated for all reporting entities every three years. At present, "cybersecurity maturity metrics" are not specifically required in state law. This bill would codify them by referencing a manual published by CDT: the Statewide Information Management Manual Section 5300-C. This bill does not provide much specific direction as to how these metrics should be adjusted to improve timeliness, but it does require the new metrics to include information from the two most recent independent security assessments performed on a state agency.

5) **Analysis.** The approach this bill outlines – requiring CDT to change the process of deriving cybersecurity maturity metrics – may not be the most preferable solution to the current problem. While slow, cybersecurity metrics play a vital role in maintaining California's cybersecurity status, as explained by CDT in the State Auditor's 2022 report:

> CDT designed the maturity metrics to be repeatable and consistent so that it can gauge each entity's progress moving forward and compare information security development across entities. For those reasons, the statewide cybersecurity metrics program manager (metrics manager) explained that CDT does not intend to change the methodology for calculating maturity metric scores during the four-year oversight life cycle. In addition to using the maturity metrics to identify gaps in a specific entity's information security, CDT uses the maturity metrics to track statewide trends that can inform the control categories for which it offers additional guidance, training, and support.

However, there may be an alternative. According to the 2022 State Auditor report, CDT requires reporting entities to meet certain self-reporting standards with respect to their information security:

1. CDT requires reporting entities to complete the federal Nationwide Cybersecurity Review (nationwide review) every year because it is a condition for receiving information security grant funding from the U.S. Department of Homeland Security. The nationwide review is a self-assessment questionnaire that reporting entities submit to the federal government. It allows entities to rate on a scale of 1 to 7 how well they are addressing different information security activities within NIST, thus providing an entity-wide information security assessment.

2. CDT also requires reporting entities to perform a security controls self-assessment based on NIST 800-53 for each of their critical IT systems to identify security risks related to that system and establish a plan to resolve those risks . . . The security controls self-assessment culminates with a high-risk findings report, which entities must submit to CDT as part of their annual Information Security and Privacy Program Compliance Certifications (compliance certifications).

3. CDT requires reporting entities to develop and maintain a Plan of Action and Milestones document (plan of action), which they must use to provide, at a minimum, quarterly

> updates to CDT on their progress toward remediating any known information security weaknesses . . . the plan of action is a document that reporting entities regularly update with information security deficiencies identified through the compliance activities we describe previously. CDT expects reporting entities to also track in their plans of action any information security weaknesses that they identify through other sources, such as security incidents or third-party oversight reviews. For each deficiency in the plan of action, reporting entities must briefly describe the high-level steps they will take to address the risk and whether they have identified any constraints to remediating the risk, among other things.[6]

In addition to these items, OIS maintains and monitors the California Compliance and Security Incident Reporting System (Cal-CSIRS). Cybersecurity incidents are reported by state entities to OIS through this system, granting OIS an up-to-date understanding of where and when attacks occur.

Taken together, CDT has access to a wealth of information reflecting the cybersecurity status of its reporting entities even in the absence of lengthy and expensive compliance audits. The State Auditor's 2022 report recommended CDT use this readily available information to more regularly estimate the security status of reporting entities:

> To ensure that it understands the statewide security status of reporting entities, CDT should do the following: . . . Utilize the information from the entities' self-assessments of their systems, as well as from the nationwide review, to annually help identify common areas that require improvement across multiple reporting entities.[7]

CDT appears to have taken this suggestion to heart. The State Auditor's 2023 report revealed that CDT has begun to develop a new "baseline information security score":

> Further, the security risk manager explained that CDT is currently developing a new priority risk ranking process that will allow it to quickly develop a baseline information security score for all reporting entities without having to complete compliance audits for each. This score will summarize readily available information, including the results of the reporting entities' independent security assessments as well as information that the reporting entities self-report annually to the federal government.[8]

The proposed committee amendments would codify the development of this baseline information security score (BISS) and require CDT to calculate a BISS for each reporting entity annually. By generating and tracking these scores over time, CDT could appropriately target its expensive, lengthy compliance audits at reporting entities found by the BISS to be particularly vulnerable.

Ultimately, adopting the BISS may be more cost effective than requiring CDT to adjust its existing maturity metric process. There are two reasons for this: first, the BISS would only

---

[6] Tilden, "The California Department of Technology's Inadequate Oversight Limits the State's Ability to Ensure Information Security," *supra.*
[7] Tilden, "The California Department of Technology's Inadequate Oversight Limits the State's Ability to Ensure Information Security," *supra.*
[8] Parks, "Weaknesses in Strategic Planning, Information Security, and Project Oversight Limit the State's Management of Information Technology," *supra.*

involve information that is already provided to or easily accessed by CDT. Second, CDT has conveyed that they are already working on developing the BISS.

6) **Proposed committee amendments.**

Section 11549.3 of the Government Code is amended to read:

(e) Before January 1, 2026, the office shall develop a Baseline Information Security Score (BISS) metric that can be used to estimate the information security status of state agencies, departments, and offices. The BISS shall utilize readily available information, including, but not limited to:

(1) Results of recent independent security assessments performed by state entities pursuant to subdivision (c).

(2) Information that state entities self-report annually to the federal government as part of the Nationwide Cybersecurity Review (NCSR).

(3) Custom reports provided to state entities by the federal government as part of NCSR.

(4) State entities' Compliance Certification and required supplementary materials, submitted pursuant to subdivision (h) paragraph (4).

(5) Any relevant incidents reported through the California Compliance and Security Incident Reporting System (Cal-CSIRS).

(6) Any recent compliance audits conducted by the Department of Technology.

(7) Any other relevant information the office possesses or is able to quickly and easily obtain.

(f) Beginning on January 1, 2027, and annually thereafter, the office shall calculate a Baseline Information Security Score for each eligible state agency, department, and office.

7) **Related legislation.** AB 1667 (Irwin, 2023) would have established the California Cybersecurity Awareness and Education Council within the Department of Technology. This bill was held on suspense in Assembly Appropriations Committee.

AB 749 (Irwin, 2023) would have required state agencies to implement Zero Trust architecture for all data, hardware, software, internal systems, and essential third-party software in order to achieve prescribed levels of maturity based on a Cybersecurity and Infrastructure Security Agency Maturity Model. This bill was held on suspense in Senate Appropriations Committee.

AB 302 (Ward, 2023) required the Department of Technology to conduct a comprehensive inventory of all high-risk automated decision systems proposed for use or procured by state agencies.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file.

Opposition

None on file.

Analysis Prepared by: Slater Sharp / P. & C.P. / (916) 319-2200