SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2021-2022 Regular Session

AB 2190 (Irwin)
Version: June 8, 2022
Hearing Date: June 21, 2022
Fiscal: Yes
Urgency: No
AM

SUBJECT

Office of Information Security: annual statewide information security status report

DIGEST

This bill requires the chief of the Office of Information Security (OIS) to submit an annual statewide information security status report including specified information to the Legislature, as provided. The bill provides that the status report and any information or records included with the status report are to be confidential and are prohibited from being disclosed, except as specified.

EXECUTIVE SUMMARY

OIS, which is within the California Department of Technology, is the principal state government authority charged with ensuring the confidentiality, integrity, and availability of state systems and applications, and ensuring the protection of state information assets. A recent report by the State Auditor found deficiencies in the way CDT oversees and ensures accountability for the compliance of state entities with information security and privacy standards issued by OIS. The Auditor's report made various recommendations to address the issues it found. This bill seeks to implement one of the Auditor's recommendations. The bill requires the chief of the Office of Information Security (OIS) to submit an annual statewide information security status report including certain information to the Legislature, provides that the report and any information or records included with the status report are to be confidential and are prohibited from being disclosed, thereby limiting the public's right to access public records. The bill makes findings to demonstrate the need for this limitation.

This bill is author sponsored. There is no known support or opposition. The bill passed the Senate Governmental Organization Committee on a vote of 14 to 0.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Establishes the Department of Technology (DOT), within the Government Operations Agency (GovOps), and generally tasks DOT 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, as specified.

2) Establishes the OIS, within DOT, for purposes of ensuring the confidentiality, integrity, and availability of state systems and applications and promoting and protecting privacy as part of the development and operations of state systems and applications, as provided.

3) Provides, pursuant to the California Constitution, that the people have the right of access to information concerning the conduct of the people's business, and, therefore, the meetings of public bodies and the writings of public officials and agencies are required to be open to public scrutiny. (Cal. Const. art. I, § 3 (b)(1).)
    a) Requires a statute that limits the public's right of access to be adopted with findings demonstrating the interest protected by the limitation and the need for protecting that interest. (Cal. const. art. I, § 3(b)(1).)

4) Governs the disclosure of information collected and maintained by public agencies pursuant to the California Public Records Act (CPRA). (Gov. Code §§ 6250 et seq.)
    a) Provides that all public records are accessible to the public upon request, unless the record requested is exempt from public disclosure. (Gov. Code § 6253.)
    b) Defines "public records" as any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics. (Gov. Code § 6252(e).)
    c) Defines "public agency" as any state or local agency. (Gov. Code § 6252(d).)
    d) Recodifies the CPRA in Division 10 of Title 1 (§§ 7920.000 - 7931.000) of the Government Code effective January 1, 2023.

This bill:

1) Requires the chief of OIS to submit an annual statewide information security status report to the Assembly Committee on Privacy and Consumer Protection and the Senate Governmental Organization Committee, as specified, that includes all of the following:
    a) the maturity metric score it has calculated for each state agency or state entity, as specified; and

b) the results of the National Cyber Security Review for each state agency and state entity, as conducted by the United States Department of Homeland Security, Multi-State Information Sharing and Analysis Center, and as available to the chief.

2) Provides that, notwithstanding any law, the status report and any information or records included with the status report are confidential and are prohibited from being disclosed; however, the information and records may be shared with members of the Legislature and legislative employees, at the discretion of the chairperson of the committee.

3) Finds that the state has a very strong interest in protecting its information technology systems from intrusion because those systems contain confidential information and play a critical role in the performance of the duties of state government. In order to protect information regarding the security status or specific vulnerabilities of those systems to preclude use of that information to facilitate attacks on those systems, it is necessary that the bill limit the public's right of access to that information.

COMMENTS

1. Stated need for the bill

The author writes:

> AB 2190 will adopt the recommendations of the State Auditor relating to the California Department of Technology from the most recent audit of the State's cybersecurity. These recommendations ensure that the Legislature is being fully informed on key cybersecurity metrics, enabling necessary oversight and investment in the State's ever evolving cybersecurity posture.

2. Ensuring information security

In January 2022, the California State Auditor (Auditor) published *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)*. 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.[1] The report noted that:

[1] Cal. State Auditor, *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)* (Jan. 18, 2022), available at https://www.auditor.ca.gov/reports/2021-602/index.html.

> 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.[2]

The Auditor's report made various recommendations to address these issues, including that the Legislature "require CDT to 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."[3] This bill seeks to implement this specific recommendation of the auditor.

3. <u>The status report is prohibited from being disclosed and is confidential</u>

Access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state. (Gov. Cod § 6250.) In 2004, the right of public access was enshrined in the California Constitution with the passage of Proposition 59 (Nov. 3, 2004, statewide gen. elec.),[4] which amended the California Constitution to specifically protect the right of the public to access and obtain government records: "The people have the right of access to information concerning the conduct of the people's business, and therefore . . . the writings of public officials and agencies shall be open to public scrutiny." (Cal. Const., art. I, sec. 3 (b)(1).) Additionally, it required a statute that limits the public's right of access to be adopted with findings demonstrating the interest protected by the limitation and the need for protecting that

[2] *Ibid*.
[3] *Ibid*.
[4] Prop. 59 was placed on the ballot by a unanimous vote of both houses of the Legislature. (SCA 1 (Burton, Ch. 1, Stats. 2004).

interest. (Cal. const. art. I, § 3(b)(1).) A public record is defined as any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any public agency regardless of physical form or characteristics. (Gov. Code § 6252(e).)

This bill limits the access to public records by prohibiting the disclosure of the statewide information security status report, and any information or records included with the status report, that the chief of OIS is required to submit to the Legislature. The bill's findings demonstrate the need for this limitation by highlighting the state's strong interest in protecting the state's information technology systems from intrusion because those systems contain confidential information and play a critical role in the performance of the duties of state government. The bill further explains that this limitation is needed to protect information regarding the security status or specific vulnerabilities of the state's information technology systems to prevent use of that information to facilitate attacks on those systems. In light of the important security and privacy issues implicated by the information in the status report, this limitation seems warranted.

SUPPORT

None known

OPPOSITION

None known

RELATED LEGISLATION

Pending Legislation:

SB 892 (Hurtado, 2022) requires OES to develop, propose, and adopt optional reporting guidelines for companies and cooperatives in the food and agriculture industry and entities in the water and wastewater systems industry if they identify a significant and verified cyber threat; and, requires OES and the California Cybersecurity Integration Center (Cal-CSIC) to prepare and submit a multiyear outreach plan to assist those sectors in their efforts to improve cybersecurity and an evaluation of options for providing grants or alternative forms of funding in their efforts to improve cybersecurity preparedness, as specified. AB 892 is pending in the Assembly Emergency Management Committee.

AB 2135 (Irwin, 2022) requires 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 requires those agencies to perform a comprehensive ISA every two years for which they

may contract with the Military Department or a qualified responsible vendor. AB 2135 is set to be heard in this Committee on the same day as this bill.

AB 1711 (Seyarto, 2022) requires that, when a person or business operating a system of records on behalf of a state or local agency is required to disclose a data breach pursuant to existing law, the state or local agency also disclose the breach by conspicuously posting the notice provided by the person or business pursuant to existing law on the agency's website, if the agency maintains one, for a minimum of 30 days. This bill is pending in the Senate Appropriations Committee.

Prior Legislation:

AB 809 (Irwin, 2021) was substantially similar to AB 2135 (Irwin, 2022). AB 809 was held in the Assembly Appropriations Committee.

AB 2408 (Smyth, Chapter 404, Statutes of 2010) codified the Governor's Reorganization Plan No. 1 of 2009 which consolidated state IT functions under the State Chief Information Officer, as specified.

PRIOR VOTES:

Senate Governmental Organization Committee (Ayes 14, Noes 0)
Assembly Floor (Ayes 74, Noes 0)
Assembly Appropriations Committee (Ayes 16, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 11, Noes 0)

****