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

AB 2135 (Irwin)
Version: April 25, 2022
Hearing Date: June 21, 2022
Fiscal: Yes
Urgency: No
AM

## SUBJECT

Information security

## DIGEST

This bill requires state agencies not under 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 independent security assessment (ISA) every two years, as specified. The bill requires those state agencies to certify annually to the Legislature, that the agency is in compliance with specified policies, standards, and procedures related to information security and privacy and provides that the certification is to be kept confidential and not disclosed, except as specifically authorized.

## EXECUTIVE SUMMARY

The Office of Information Security (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 California State Auditor (Auditor) highlighted continued issues related to non-reporting entities' information security, i.e. state agencies not under direct authority of the Governor. This bill seeks to ensure information security across all state entities by requiring non-reporting agencies to adopt information security and privacy policies, standards, and procedures meeting specified federally-established criteria and requires those entities to perform an ISA every two years. The bill requires those state agencies to certify to the leadership of the Legislature that the agency is in compliance with these requirements.

The 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 Office of Information Security (OIS), within the Department of Technology (CDT), for the purpose of ensuring 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 the residents of this state, as specified.

2) Requires state agencies and state entities within the executive branch that are under the direct authority of the Governor to implement the policies and procedures issued by OIS, as specified.

3) Authorizes OIS to conduct, or require to be conducted, an ISA of every state agency, department, or office, as specified, and authorizes the California Military Department (CMD) to perform an ISA of any state agency, department, or office, a specified.

4) 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).)

5) 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 every state agency not subject to existing information security standards, practices, and procedures issued by 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) Requires state agencies not under direct authority of the Governor to perform a comprehensive ISA every two years, as specified.

3) Authorizes state agencies not under direct authority of the Governor to contract with CMD, or with a qualified responsible vendor, to perform an ISA, as specified.

4) Requires state agencies not under direct authority of the Governor to certify, by February 1 annually, to the President pro Tempore of the Senate and the Speaker of the Assembly, that the agency is in compliance with all policies, standards, and procedures adopted pursuant to this bill. The certification is required to include a plan of action and milestones, as specified.

5) Notwithstanding any other law, provides that the certification shall be kept confidential and shall not be disclosed, except that the information and records may be shared, maintaining a chain of custody, with the members of the Legislature and legislative employees, at the discretion of either the President pro tempore of the Senate or the Speaker of the Assembly.
    a) Requires legislative leadership to consult with the state agencies described above on the policies and procedures for transferring, receiving, possessing, or disclosing certifications that ensure confidentiality and security of the certification, as specified.

6) Provides that this bill only applies to the University of California (UC) if the Regents of the UC, by resolution, make any of the provisions of the bill applicable to the UC.

## COMMENTS

1. Stated need for the bill

The author writes:

> The results of this year's high risk audit, raising the alarm once again on "non-reporting" entity's cybersecurity, are an important reminder of the urgency for the Legislature to act and ensure these offices adopt standards and be subject to external oversight to prioritize securing their networks. The Legislature must step in as the Auditor recommends and ensure that information security

> standards are adopted by Constitutional Officers and other independent offices within state government. The time of ignoring our vulnerabilities to cyber-attacks passed long ago, and its time all of state government is on the same page about cybersecurity.

2. Ensuring information security and non-reporting entities

*a. Non-reporting entities*

Existing law requires all state entities to 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 § 11549.3(a).) Existing state law also authorizes OIS to conduct an information security audit (ISA), or require and ISA to be conducted, of every state agency, department, or office. (Gov. Code § 11549.3(b).) The use of different terms under these statutes—*state agency* versus *every state agency, department, or office*—has led to uncertainty about which state entities are subject to these requirements, and several state entities have asserted that they are not subject to these requirements. This includes non-reporting state agencies, i.e. state entities that are not under the direct authority of the Governor and therefore do not report to the Governor, such as constitutional officers, which are Executive Branch officers specifically provided for by the California Constitution.[1]

*b. Auditor's report and recommendation*

In January 2022, the 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.[2] However, the report noted that:

> [W]hen we surveyed 32 nonreporting entities, we found that they also have not adequately addressed their information security. Although 29 of the 32 nonreporting entities have adopted an information security framework or standards, only four reported that they had achieved full compliance with their chosen framework or standards. […] In our previous report, we identified gaps in oversight that have contributed to nonreporting entities' information security

[1] Constitutional officers include 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.
[2] 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.

> weaknesses. [citation omitted] We also noted that some non-reporting entities have an external oversight framework that requires them to assess their information security regularly. We found that nonreporting entities with external oversight were generally further along in their information security development than those without such oversight. Given the value of external oversight of information security and considering our recent survey results, the Legislature should create an oversight structure for all nonreporting entities.[3]

The Auditor's report recommended that state law be amended to "require each non-reporting entity to adopt information security standards comparable to those required by CDT and to provide a confidential, annual status update on its compliance with its adopted information security standards to legislative leadership, including the president pro tempore of the California State Senate, the speaker of the California State Assembly, and minority leaders in both houses.[4]"

*c. This bill seeks to resolve any uncertainty under the law and ensure information security across all state entities*

This bill seeks to resolve any uncertainty under the law and ensure information security across all state entities by specifically applying OIS information security standards and ISA requirements to non-reporting entities. The bill requires non-reporting entities to certify annually to the President pro Tempore of the Senate or the Speaker of the Assembly that the agency is in compliance with OIS policies, standards, and procedures related to information security and privacy. The bill provides that the certification is to be kept confidential and not disclosed, except the information and records may be shared, maintaining a chain of custody, with the members of the Legislature and legislative employees, at the discretion of either the President pro tempore of the Senate or the Speaker of the Assembly.

*d. Prior bills that attempted to address the issue of non-reporting entities complying with OIS standards and ISAs*

There were several prior bills that sought to address this issue, but they were never enacted. AB 809 (Irwin, 2021) was substantially similar to this bill and was held in the Assembly Appropriations Committee. AB 2669 (Irwin, 2020) was substantially similar to AB 809 and was not set for a hearing in the Assembly Committee on Privacy and Consumer Protection due to constraints on the legislative processes imposed by the COVID-19 pandemic. AB 3193 (Chau, 2018) attempted to require non-reporting agencies to comply with OIS standards and ISAs by amending an existing definition of state agency to include constitutional officers and other non-reporting entities. AB 3193

---

[3] 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) at pp. 2-3, available at https://www.auditor.ca.gov/reports/2021-602/index.html.
[4] *Id.* at 3.

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.

3. The certification provided to legislative leadership is prohibited from being disclosed and is considered confidential

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.),[5] 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 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 the certification made to legislative leadership by prohibiting its disclosure. 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 certification, this limitation seems warranted.

**SUPPORT**

None known

**OPPOSITION**

None known

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

## RELATED LEGISLATION

Pending Legislation:

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.

AB 2190 (Irwin, 2022) requires that CDT confidentially submit an annual statewide information security status report, including specified information, to the Chair of the Assembly Committee on Privacy & Consumer Protection and the Chair of the Senate Governmental Organization Committee. AB 2135 is set to be heard in this Committee on the same day as this bill.

Prior Legislation:

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

AB 2669 (Irwin, 2020) was substantially similar to AB 809 (Irwin, 2021). AB 2669 was not set for a hearing in the Assembly Committee on Privacy and Consumer Protection.

AB 3193 (Chau, 2018) would have required all state agencies, including constitutional officers and other non-reporting entities, to comply with security and privacy policies and incident notification requirements established by OIS, and to undergo mandatory ISAs. AB 3193 died in the Senate Governmental Organization Committee.

AB 670 (Irwin, Ch. 518, Stats. 2015) authorized OIS to conduct, or require to be conducted, an ISA of every state agency, department, or office, as specified.

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 76, Noes 0)
Assembly Appropriations Committee (Ayes 16, Noes 0)
Assembly Accountability and Administrative Review Committee (Ayes 7, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 11, Noes 0)

**********