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

AB 1352 (Chau)
Version: March 22, 2021
Hearing Date: July 6, 2021
Fiscal: Yes
Urgency: No

SUBJECT

Independent information security assessments: Military Department: local educational agencies

DIGEST

This bill permits a local educational agency (LEA) to engage the California Military Department to perform an independent security assessment of the LEA's information security, or the information security of an individual schoolsite within the LEA.

EXECUTIVE SUMMARY

California's schools are increasingly reliant on information technology, and particularly online programs and platforms. The COVID-19 pandemic accelerated this reliance, as schools across the state moved to remote online instruction. This bill seeks to strengthen the security of LEA's information technology and protections against threats such as ransomware by allowing an LEA to request the California Military Department to perform and independent security assessment of the LEA's information security, or the information security of individual schools within the LEA, to be paid for by the LEA. The bill provides that the results of the assessment will be disclosed only to the LEA and may not be disclosed under the California Public Records Act (CPRA).

This bill was originally triple referred to the Senate Committees on Military and Veterans Affairs, Judiciary, and Education. The referral to the Senate Education Committee was rescinded because of the limitations placed on committee hearings due to the ongoing health and safety risks of the COVID-19 virus, and this analysis includes input from the Senate Education Committee on the matters within its jurisdiction.

This bill is sponsored by the author and supported by California IT in Education. There is no known opposition. This bill passed out of the Senate Military and Veterans Affairs Committee with a vote of 6-0.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Establishes the Office of Information Security (OIS) within the Department of Technology. The OIS's purpose is to ensure the confidentially, 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. (Gov. Code, § 11549(a).)

2) Provides that the OIS is led by a chief, whose duties include providing direction for information security and privacy to state government agencies, departments, and offices. (Gov. Code, § 11549(b).)

3) Requires the chief to establish an information security program, the responsibilities of which include:
    a) The creation, updating, and publishing of information security and privacy policies, standards, and procedures for state agencies in the State Administrative Manual.
    b) The creation, issuance, and maintenance of policies, standards, and procedures directing state agencies to effectively manage security and risk for information technology, as defined, and information identified as mission critical, confidential, sensitive, or personal, as defined and published by the LIS.
    c) The creation, issuance, and maintenance of policies, standards, and procedures directing state agencies for the collection, tracking, and reporting of information regarding security and privacy incidents.
    d) The creation, issuance, and maintenance of policies, standards, and procedures directing state agencies in the development, maintenance, testing, and filing of each state's disaster recovery plan.
    e) Coordination of the activities of state agency information security officers, for purposes of integrating statewide security initiatives and ensuring compliance with information security and privacy policies and standards.
    f) Promotion and enhancement of the state agencies' risk management and privacy programs through education, awareness, collaboration, and consultation.
    g) Representing the state before the federal government, other state agencies, local government agencies, and private industry on issues that have statewide impact on information security and privacy. (Gov. Code, § 11549.3(a).)

4) Requires specified state entities to implement the policies and procedures issued by the OIS, including complying with the OIS's information security and privacy policies, standards, and procedures and complying with filing requirements and

incident notification by providing timely information and reports as required by the OIS. (Gov. Code, § 11549.3(b).)

5) Permits the OIS to conduct, or require to be conducted, an independent security assessment of every state agency, department, or office, with the cost of the assessment funded by the agency, department, or office being assessed. The OIS must annually require no fewer than 35 state entities to perform such an assessment, and must determine criteria and rank state entities based on an information security risk index that may include analysis of factors including (1) the amount of personally identifiable information protected by law, (2) the amount of health information protected by law, (3) confidential financial data, and (4) self-certification of compliance and indicators of unreported compliance with security provisions in specified areas. (Gov. Code, § 11549.3(c)(1)-(2).)

6) Permits the Military Department to perform an independent security assessment of any state agency, department, or office, the cost of which shall be funded by the state agency, department, or office being assessed. (Gov. Code, § 11549.3(c)(3).)

7) Requires state agencies and entities required to conduct or receive an independent security assessment to transmit the complete results and recommendations for mitigating system vulnerabilities, if any, to the OIS and the Office of Emergency Services. (Gov. Code, § 11549.3(d).)

8) Requires the OIS to report to the Departments of Technology and Emergency Services any state entity found to be noncompliant with information security program requirements. (Gov. Code, § 11549.3(e).)

9) Provides the following with respect to information security assessment information:
    a) During the process of conducting an independent security assessment, information and records concerning the assessment are confidential and shall not be disclosed, except that the information and records may be transmitted to approved state employees and contractors as necessary to receive the information and records to perform the assessment, subject to remediation activity or monitoring of remediation activity.
    b) The results of a completed independent security assessment and any related information are subject to all disclosure and confidentially provisions pursuant to state law, including the California Public Records Act (CPRA). (Gov. Code, § 11549.3(f).

10) Establishes the CPRA, which generally makes public records available for inspection unless exempted from disclosure. (Gov. Code, tit. 1, div. 7, ch. 3.5, art. 1, §§ 6250 et seq.)

11) Establishes an exemption to disclosure of public records under the CPRA for information security records of a public agency if, on the facts of the particular case,

> the disclosure would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency. This exemption does not limit the disclosure of public records stored within an information technology system of a public agency that are not otherwise exempt from disclosure. (Gov. Code, § 6254.19.)

This bill:

1) Defines "local educational agency" to mean a school district, county office of education, charter school, or state special school.

2) Authorizes the Military Department, at the request of a local educational agency, to perform an independent security assessment of the local educational agency, or an individual schoolsite under its jurisdiction, the cost of which shall be funded by the local educational agency.

3) Provides that the criteria for the LEA independent security assessment shall be established by the Military Department in coordination with the LEA.

4) Requires the Military Department to disclose the results of the independent security assessment only to the LEA.

5) Provides that the results of the independent security assessment and related information are exempt from disclosure under applicable state law, including the CPRA's exemption for information security records of a public agency.

COMMENTS

1. Author's comment

According to the author:

> Cybersecurity threats are a common reality today that have become an important consideration for governmental entities throughout the State. For example, to protect the integrity of our elections, the Secretary of State has an Office of Election Cybersecurity to counter online interference in our elections.[1] Since 2015, the California Cybersecurity Integration Center, or "Cal-CSIC" - an interdisciplinary and interdepartmental organization - has also served a leading role is our State's cybersecurity strategy.
>
> Further, the 2020-21 budget made important investments in cybersecurity: $11.1 million to various department to enhance the state's critical cybersecurity

[1]California Secretary of State, *Election Cybersecurity*, www.sos.ca.gov/elections/election-cybersecurity [last visited Jul. 2, 2021].

infrastructure, including $7.6 million to the Office of Emergency Services; and $2.9 million to protect patient health records with strengthened cybersecurity infrastructure. Simply put, California has committed to expanding and enhancing the government's cybersecurity posture.

To close education equity gaps, LEAs have heavily invested in new technology for their instruction. For example, last year, LAUSD spent $100 million on Chromebooks and iPads.[2] However, increased reliance on technology comes with heightened cybersecurity risks. According to a Microsoft Security Intelligence report, the education sector suffered the majority of cyber-attacks in 30 days between May and June 2020.[3]

This bill is necessary to ensure the state government is affording its LEAs an effective way to identify and address threats to their cybersecurity. As schools increasingly depend on computerized systems to deliver instruction, the risk of cybersecurity problems will heighten. Thus, it is sensible for the Legislature to authorize the Military Department to be a cybersecurity partner for LEAs.

2. <u>This bill provides LEAs with the option of requesting the Military Department to perform an independent security assessment of the LEA's cybersecurity</u>

Society's increased reliance on the internet has led to greater connectivity and ways of engaging with each other, but it has also led to greater opportunities for cybercrime. Every login for every service is a potential access point for a hacker; every user in a network who might click on an unknown link is a potential malware downloader.

With many schools moving to remote or partially remote instruction due to the COVID-19 virus, schools have become a primary target for cyberattacks. Microsoft Security Intelligence, which keeps a running tracker of malware encounters, reports that over 63 percent of malware encounters in the last 30 days were in the education sector.[4] Ransomware attacks against schools also spiked in 2020; the Federal Bureau of Investigation estimates that 57 percent of ransomware attacks on state, local, and tribal entities in August and September 2020 were against kindergarten through grade 12 institutions, up from 28 percent in January through July 2020.[5] Schools often make

---

[2] Stokes, *In LAUSD, 'Just About Every' Student Now Has A Laptop To Use During The Pandemic*, LAist (Mar. 11, 2020) https://laist.com/2020/05/11/lausd_schools_laptop_chromebook_ipad_distribution_complete_beutner_update.php [last visited Jul. 2, 2021].

[3] Castelo, *Cyberattacks Increasingly Threaten Schools – Here's What to Know*, EdTech (Jun. 17, 2020) https://edtechmagazine.com/k12/article/2020/06/cyberattacks-increasingly-threaten-schools-heres-what-know-perfcon [last visited Jul. 2, 2021].

[4] Microsoft Security Intelligence, *Global Threat Activity* (as of June 18, 2021), https://www.microsoft.com/en-us/wdsi/threats [last visited Jul. 2, 2021].

[5] Marks, *The Cybersecurity 202: Spiking ransomware attacks against schools make pandemic education even harder*, Washington Post (Dec. 20, 2020),

tempting targets because (1) they have had to adopt new online technologies on the fly due to COVID-19, (2) many have budgetary constraints that prevent the adoption of adequate cybersecurity systems, and (3) they are more likely than other organizations to have insurance companies that will pay out in the event of a ransomware attack.[6]

The California state government has an office—the OIS—dedicated to ensuring security of the state's information technology systems and the confidentially of private information held by the state (e.g., employee information).[7] The OIS and the Military Department are authorized to conduct independent security assessments of state agencies, departments, and offices, paid for by the subject of the assessment.[8] There is no similar provision, however, allowing the OIS or the Military Department to conduct independent security assessments of LEAs.

This bill authorizes an LEA to request that the Military Department perform an independent security assessment of the LEA, or an individual schoolsite within the LEA's jurisdiction. The LEA and the Military Department will coordinate on the criteria for the assessment, and the LEA will fund the cost of the assessment. Once the assessment is complete, the Military Department will provide the results only to the LEA, which will then be able to use the results as a roadmap for how to enhance its cybersecurity measures.

3. <u>This bill renders the results of an LEA's security assessment confidential and not subject to disclosure under the CPRA</u>

This bill provides that the results of a Military Department independent security assessment will stay confidential, with two provisions. First, it provides that the Military Department will provide the results of the assessment only to the LEA. Second, it provides that the results of the assessment are subject to the confidentiality provisions of state law, including the CPRA's disclosure exemption for information security records.[9] This exemption provides that information security records need not be disclosed where, on the facts of the particular case, disclosure "would reveal vulnerabilities to, or increase the potential for an attack on, the information technology system of a public agency."[10] The statute clarifies that it does not render otherwise-disclosable information confidential simply because the record is stored within an information technology system.[11]

---

https://www.washingtonpost.com/politics/2020/12/11/cybersecurity-202-spiking-ransomware-attacks-against-schools-make-pandemic-education-even-harder/ [last visited Jul. 2, 2021].
[6] *Ibid.*
[7] Gov. Code, §§ 11549, 11549.3.
[8] *Id.*, § 11549.3(c).
[9] *See* Gov. Code, § 6254.19.
[10] *Ibid.*
[11] *Ibid.*

While the provision is not absolute—it is conceivable that a court could conclude that a particular assessment would not pose a security threat if disclosed—it appears to squarely apply to the security assessments set forth in this bill. Existing law already provides that the results of independent security assessments performed by the Military Department or OIS for a state agency are covered by this CPRA exemption;[12] it therefore seems consistent to apply the same degree of confidentiality to the results of assessments performed for LEAs. Moreover, because the entire purpose of the bill is to help LEAs discover shortcomings in their information security systems, it seems highly likely that the results will contain information that would increase the likelihood of cyberattacks if disclosed to the public.

4. Comment from the Senate Education Committee

According to the Senate Education Committee:

> **Education and technology.** The COVID-19 pandemic laid bare education's dependence on technology. This integral relationship includes a multitude of networks, internet web sites and portals, data systems, and devices, both on campus and off, across a variety of local educational agencies and state entities. Local educational agencies and individual schools possess sensitive personal information protected by both state and federal privacy laws. As more local educational agencies provide devices to students for home use that remain connected to networks, more potential pathways for intrusion are created. To the extent that Independent Security Assessments can help local educational agencies mitigate these vulnerabilities and navigate cybersecurity dangers, they could be a valuable tool.

5. Arguments in support

According to bill supporter California IT in Education:

> The use of technology in our schools was already rapidly expanding before the COVID-19 pandemic. Everything from payroll, to digital and online curricula, to HVAC systems; schools rely on technology for day-to-day operations. Unfortunately, with this increase in technology usage has come a similar increase in cybersecurity threats. In particular, there has been a marked increase in ransomware attacks and phishing schemes. This problem has only become more exacerbated by the COVID-19 pandemic. To ensure students continue to receive high-quality educations, schools across the state have worked diligently to rapidly deploy distance learning models. However, as networks expanded, so too did cybersecurity threats.

[12] Gov. Code, § 11549.3(f)(2).

While many schools are reopening for in-person instruction, it is unlikely these threats will abate. The first step to helping mitigate these threats is identifying vulnerabilities. Unfortunately, having a private or third-party entity perform a cybersecurity audit can be extremely costly. Many LEAs simply do not have the resources to either accurately assess their networks, or contract with an agency to do so. AB 1352 will help solve this problem by allowing an LEA to request the Military Department—which is already responsible for auditing state-level agencies and well equipped to do this work—to perform an independent cybersecurity audit of its technology infrastructure. Further, the bill makes it clear that the LEA can work collaboratively with the Military Department on the parameters of the audit, and that the findings of the audit only be disclosed to the LEA.

SUPPORT

California IT in Education

OPPOSITION

None known

RELATED LEGISLATION

Pending Legislation:

AB 809 (Irwin, 2021) implements recommendations of the California State Auditor contained in Report 2018-611 "Gaps in Oversight Contribute to Weaknesses in the State's Information Security" released in July 2019 relating to agencies not currently governed by the OIS. AB 809 was held on the Assembly Appropriations Committee suspense file.

AB 581 (Irwin, 2021) would require all state agencies, as generally defined, to review and implement specified National Institute of Standards and Technology (NIST) guidelines for, among other things, reporting, coordinating, publishing, and receiving information about a security vulnerability relating to information systems and the resolution thereof, no later than July 1, 2022, and require the chief to review the NIST guidelines and to create, update, and publish any appropriate standards or procedures in the State Administrative Manual and Statewide Information Management Manual to apply the NIST guidelines to certain state governmental agencies, as defined, no later than April 1, 2022. AB 581 was held on the Assembly Appropriations Committee suspense file.

Prior Legislation:

AB 2669 (Irwin, 2020) would have required state agencies not falling under the jurisdiction of the OIS to adopt and implement information security and privacy policies, standards, and procedures based upon standards issued by the National Institute of Standards and Technology and the Federal Information Processing Standards, as specified, and to perform a comprehensive, independent security assessment every two years and would authorize them to contract with the Military Department for that purpose. AB 2669 died in the Assembly Privacy and Consumer Protection Committee.

AB 1242 (Irwin, 2019) would have expanded the state entities falling under the jurisdiction of the OIS with respect to information security. AB 1242 died in the Assembly Appropriations Committee.

AB 3193 (Chau, 2018) would have expanded the state entities falling under the jurisdiction of the OIS with respect to information security. AB 3193 died in the Senate Governmental Organization Committee.

AB 531 (Irwin, 2017) would have required the OIS, on or before July 1, 2019, to review information security technologies currently in place in state agencies to determine if there are sufficient policies, standards, and procedures in place to protect critical government information and prevent the compromise or unauthorized disclosure of sensitive digital content, as defined, inside or outside the firewall of state agencies, and following the review, to develop a statewide plan to require the implementation by state agencies of any information security technology OIS determined to be necessary to protect critical government information and prevent the compromise or unauthorized disclosure of sensitive digital content of a state agency. AB 531 was vetoed by Governor Edmund G. Brown, Jr., whose veto message stated that the bill's objectives were already being fulfilled by required security assessments in process.

AB 670 (Irwin, Ch. 518, Stats. 2015) required the OIS to conduct no fewer than 35 independent security assessments annually and to report to the Department of Technology and Office of Emergency Services any state entity not in compliance with information security requirements.

PRIOR VOTES:

Senate Military and Veterans Affairs Committee (Ayes 6, Noes 0)
Assembly Floor (Ayes 76, Noes 0)
Assembly Appropriations Committee (Ayes 16, Noes 0)
Assembly Military and Veterans Affairs Committee (Ayes 11, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 11, Noes 0)

****