

## CONCURRENCE IN SENATE AMENDMENTS

AB 1352 (Chau)

As Amended August 24, 2021

Majority vote

**SUMMARY**

This bill authorizes the Military Department to perform an independent security assessment (ISA) of a local educational agency (LEA) or schoolsite, at the request and expense of the LEA.

**Senate Amendments**

- 1) Provide that an ISA performed by the Military Department at the request of a LEA shall be performed in consultation with the California Cybersecurity Integration Center.
- 2) Specify that the results of the ISA shall be disclosed to the California Cybersecurity Integration Center, in addition to the LEA.

**COMMENTS**

An ongoing analysis by Microsoft Security Intelligence indicates that over the last 30 days (as of September 1, 2021), the education sector experienced over 63% of all enterprise malware encounters worldwide, amounting to nearly 6 million devices. The next closest sector, the business and professional services sector, accounts for only 9% of detected malware encounters, and fewer than 1 million devices. The increasing cyber vulnerability of schools has likely in part resulted from the ever-increasing sophistication of malicious actors, and in part from increased adoption of digital infrastructure for both educational purposes and school administration. The COVID-19 pandemic has only accelerated this transition to digital infrastructure, as adoption of digital educational tools has been essential to facilitate the remote learning environment necessitated by efforts to combat the pandemic.

Cyberattacks on schools are particularly harmful, as they have the potential to interfere with a school's educational mission by prohibiting normal instruction, and can also result in the unauthorized disclosure of highly sensitive pupil records. Both state and federal law recognize the unique sensitivity of pupil records, and place stringent limitations on conditions in which such information can be disclosed.

Acknowledging the pressing cybersecurity issues facing this State and, in particular, the State's public agencies, California has in recent years invested heavily in the security of its information technology (IT) infrastructure. In 2015, Executive Order B-34-15 required the Office of Emergency Services to establish and lead the California Cybersecurity Integration Center (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, and was codified three years later by AB 2813 (Irwin), Chapter 768, Statutes of 2018.

In 2010, the Legislature passed AB 2408 (Smyth), Chapter 404, Statutes of 2010, which, among other things, required the chief of the Office of Information Security (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. Five years later, the Legislature expanded on the authority of OIS by passing AB 670 (Irwin), Chapter 518, Statutes of 2015, which authorized OIS to conduct, or require to be conducted, an ISA of 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, annually require no fewer than 35 state entities to conduct an ISA. AB 670 allowed these ISAs to be conducted by the Military Department, which serves a principal role on 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)(3).)

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 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 3<sup>rd</sup> 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].

Notably, while AB 670 authorized OIS to require, and the Military Department to conduct, ISAs of any state agency, department, or office, it did not address the availability of these services to local agencies, including LEAs. Consequently, despite their critical function and vulnerability to cyberattack, LEAs cannot, under existing law, utilize the State's expertise in assessing and improving the cybersecurity of their IT infrastructure. Instead, if an LEA opts to undergo such an assessment at all, they must rely on costly, for-profit third-party services that may themselves fail to meet the stringent cybersecurity standards the State maintains for its own networks.

*This bill* would allow LEAs to request that the Military Department perform an ISA of the LEA or a specific schoolsite within its jurisdiction, in order to allow LEAs to avail the state's cybersecurity expertise and protect their critical IT infrastructure.

Under existing law, an ISA of a state agency, department, or office, that is conducted by the Military Department is carried out at the behest of OIS, and in accordance with criteria established by OIS. The cost of the assessment is furnished by the agency, department, or office being assessed. AB 1352 would permit an LEA to request that the Military Department conduct an ISA of the LEA or an individual schoolsite under its jurisdiction, but would under no circumstances require an LEA to undergo an ISA. While the cost of the ISA would similarly be furnished by the LEA, the criteria for that ISA would be established by the Military Department in coordination with the LEA itself, rather than being based strictly on the criteria established by OIS. The bill is also permissive rather than obligatory with respect to the Military Department's compliance with any such request by an LEA so as to permit appropriate triage of ISA requests

based on the relative risk and the personnel and other resources the Military Department has available. The bill would define "local educational agency" to include a school district, county office of education, charter school, or state special school.

While LEAs likely face many of the same cybersecurity threats as state agencies, there are some critical differences between their circumstances that seemingly necessitate the permissiveness AB 1352 provides with respect to ISAs. First, generally speaking, LEAs typically serve a diverse set of roles within a community. Though LEAs are primarily focused on their core educational mission, they must also coordinate extracurricular services, including afterschool programs, competitive sports, school lunch programs, and many broader community functions. The extent to which a given LEA prioritizes any one of these services, and even the extent to which they prioritize specific educational objectives, can vary greatly between localities based on the particular needs of that student body, and that community as a whole. Though the State tends to be fairly prescriptive with respect to the practicalities of agency function, by design, there is a great deal of local independence provided for LEAs in order to meet the specific needs of their communities. Consequently, the criteria appropriate for an ISA will likely vary depending on the role IT plays in that particular LEA's objectives and practices, and depending on the resources that LEA has available to allocate to assessing cybersecurity risks. While one LEA may have ample discretionary funds to contribute to a highly comprehensive and sophisticated ISA, another may not, but should nonetheless be able to coordinate an assessment of their security practices to the extent available.

Second, LEAs are generally operating on shoestring budgets, with minimal surplus funds to allocate toward the hiring of specialized staff to manage information security. Though OIS develops and enforces certain standards and practices for information security with which state agencies must comply, these agencies are generally budgeted the necessary funds for compliance, and thus retain staff with subject expertise to oversee information security practices. The head of each state agency is also required to appoint a chief information officer to "oversee the information technology portfolio and information technology services within [the] state agency, as well as an information security officer. (Gov. Code Sec. 11546.1(a)-(c).) In contrast, the budgets for LEAs typically lack earmarked funds for such needs, and there is no requirement that LEAs retain staff specifically to oversee information security. Without this onsite expertise, an LEA interested in strengthening cybersecurity would most likely need to secure the services of a private third-party with appropriate expertise, which could be costly and potentially substandard. By providing LEAs with the opportunity to avail the services of the Military Department in conducting an ISA, they can ensure that the services are incurred at cost, i.e., without markup, and that the services meet state standards, including confidentiality, as AB 1352 explicitly limits disclosure of the results of an ISA to the LEA itself, along with the California Cybersecurity Integration Center. Though it is true that the LEA would still be responsible for covering the expense of the assessment, by providing ISAs only at the request of the LEA, AB 1352 allows a given LEA more discretion over how they allocate funding to best protect the interests of their students, and the priority cybersecurity plays in that objective.

In providing LEAs with a mechanism to effectively identify specific points of vulnerability and solicit recommendations for improvements, AB 1352 would seem to allow for LEAs to more efficiently target the limited funds allocated for the purpose of information security by prioritizing resolution of the vulnerabilities posing the highest immediate risk. This would presumably increase the likelihood that schools resolve outstanding cybersecurity shortcomings

in a timely manner to better protect sensitive pupil records and the essential capacity for schools to achieve their educational goals.

**According to the Author**

Over the past year, the pandemic has forced many governmental entities to shift many in-person operations online. Perhaps the entities that have experienced this shift more dramatically than any others are California's LEAs, when schools were forced to instantaneously shift from in-class learning to remote learning. [...] As California's schools become more reliant on computer systems, their need to effectively identify cybersecurity shortcomings will only heighten.

Pursuant to Government Code Section 11549.3, the Military Department coordinates with other state departments in maintaining an information security program. Through this program, it assists in conducting independent security assessments of state agencies, departments, and offices. Given its experience in assessing security risks for state government, the Military Department makes a sensible partner for LEAs in enhancing their cybersecurity. [T]his bill would allow an LEA to engage the California Military Department to perform an independent security assessment of the LEA, or an individual schoolsite under the jurisdiction of the LEA, the cost of which shall be funded by the LEA.

**Arguments in Support**

California IT in Education (CITE) argues:

The usage 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 was only exacerbated by the COVID-19 pandemic. To ensure students continued to receive high-quality educations, schools across the state worked diligently to rapidly deploy distance learning models. However, as networks expanded, so too, did cybersecurity threats.

While students will be returning to in-person instruction in the fall, 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.

**Arguments in Opposition**

None on file

**FISCAL COMMENTS**

According to the Assembly Appropriations Committee, no costs to the CMD, given that any security assessment would have to be funded by the school district that requests the cybersecurity assessment.

**VOTES:****ASM PRIVACY AND CONSUMER PROTECTION: 11-0-0**

**YES:** Chau, Kiley, Bauer-Kahan, Bennett, Carrillo, Cunningham, Gabriel, Gallagher, Irwin, Lee, Wicks

**ASM MILITARY AND VETERANS AFFAIRS: 11-0-0**

**YES:** Irwin, Voepel, Boerner Horvath, Daly, Frazier, Mathis, Muratsuchi, Petrie-Norris, Ramos, Salas, Smith

**ASM APPROPRIATIONS: 16-0-0**

**YES:** Lorena Gonzalez, Bigelow, Calderon, Carrillo, Chau, Megan Dahle, Davies, Fong, Gabriel, Eduardo Garcia, Levine, Quirk, Robert Rivas, Akilah Weber, Friedman, Stone

**ASSEMBLY FLOOR: 76-0-2**

**YES:** Aguiar-Curry, Arambula, Bauer-Kahan, Bennett, Berman, Bigelow, Bloom, Boerner Horvath, Burke, Calderon, Carrillo, Cervantes, Chau, Chen, Chiu, Choi, Cooley, Cooper, Megan Dahle, Daly, Davies, Flora, Fong, Frazier, Friedman, Gabriel, Gallagher, Cristina Garcia, Eduardo Garcia, Gipson, Lorena Gonzalez, Gray, Grayson, Holden, Irwin, Jones-Sawyer, Kiley, Lackey, Lee, Levine, Low, Maienschein, Mathis, Mayes, McCarty, Medina, Mullin, Muratsuchi, Nazarian, Nguyen, O'Donnell, Patterson, Petrie-Norris, Quirk, Quirk-Silva, Ramos, Reyes, Luz Rivas, Robert Rivas, Rodriguez, Blanca Rubio, Salas, Santiago, Seyarto, Smith, Stone, Ting, Valladares, Villapudua, Voepel, Waldron, Ward, Akilah Weber, Wicks, Wood, Rendon

**ABS, ABST OR NV:** Cunningham, Kalra

**SENATE FLOOR: 39-0-1**

**YES:** Allen, Archuleta, Atkins, Bates, Becker, Borgeas, Bradford, Caballero, Cortese, Dahle, Dodd, Durazo, Eggman, Glazer, Gonzalez, Grove, Hertzberg, Hueso, Hurtado, Jones, Kamlager, Laird, Leyva, Limón, McGuire, Melendez, Min, Newman, Nielsen, Ochoa Bogh, Pan, Portantino, Roth, Rubio, Skinner, Umberg, Wieckowski, Wiener, Wilk

**ABS, ABST OR NV:** Stern

**UPDATED**

VERSION: August 24, 2021

CONSULTANT: Landon Klein / P. & C.P. / (916) 319-2200

FN: 0001580