Date of Hearing: April 8, 2021

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 1352 (Chau) – As Amended March 22, 2021

**SUBJECT**: Independent information security assessments: Military Department: local educational agencies

**SUMMARY**: This bill would authorize 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. Specifically, **this bill would**:

1) Authorize the Military Department to perform an ISA of an LEA, or of an individual schoolsite under the jurisdiction of an LEA, at the LEA's request, the cost of which shall be funded by the LEA.

2) Provide that the criteria for the ISA shall be established by the Military Department in coordination with the LEA.

3) Specify that the Military Department shall disclose the results of the ISA only to the LEA.

**EXISTING LAW**:

1) Establishes, within the Government Operations Agency, the Department of Technology, and generally tasks the department 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. (Gov. Code Sec. 11545, et seq.)

2) Establishes, within the Department of Technology, the Office of Information Security (OIS), with the purpose of ensuring the confidentiality, integrity, and availability of state IT systems and promoting and protecting privacy as part of the development and operations of state IT systems, and tasks OIS with the duty to provide direction for information security and privacy to state government agencies, departments, and offices. (Gov. Code Sec. 11549(a) and (c).)

3) Requires the chief of OIS to establish an information security program with responsibilities including, among others, 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. (Gov. Code Sec. 11549.3(a).)

4) Authorizes OIS to conduct, or require to be conducted, an ISA of every state agency, department, or office, the cost of which shall be funded by the state agency, department, or office being assessed, and specifies that OIS must, in consultation with the Office of Emergency Services, annually require no fewer than 35 state entities to perform an ISA. (Gov. Code Sec. 11549.3(c)(1) and (2).)

5) Authorizes the Military Department to perform an ISA of any state agency, department, or office, the cost of which shall be funded by the agency, department, or office being assessed. (Gov. Code Sec. 11549.3(c)(3).)

6) Specifies that, notwithstanding any other law, during the process of conducting an ISA, information and records concerning the ISA are confidential and shall not be disclosed, except to state employees or contractors who have been approved as necessary to receive the information and records to perform the ISA or subsequent remediation activity, and that the results of a completed ISA are subject to all applicable laws relating to disclosure and confidentiality including the California Public Records Act. (Gov. Code Sec. 11549.3(f).)

7) Provides that nothing in the California Public Records Act shall be construed to require the disclosure of an information security record of a public agency, if, on the facts of the particular case, disclosure of that record would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency. (Gov. Code Sec. 6254.19.)

8) Authorizes an LEA to enter into a contract with a third party to provide services, including cloud-based services, for the digital storage, management, and retrieval of pupil records, or to provide digital educational software that authorizes a third-party provider to access, store, and use pupil records. (Ed. Code Sec. 49073.1(a).)

9) Specifies numerous conditions and limitations on the use, maintenance, and disclosure or release of pupil records and information by an LEA, including prohibiting a school district from permitting access to pupil records to a person without written parental consent or a lawfully issued subpoena or court order to do so. (Ed. Code Sec. 49073, et seq.)

**FISCAL EFFECT**: Unknown

**COMMENTS**:

**1) Purpose of this bill**: As California's educational institutions become increasingly reliant on IT for essential functions, this bill seeks to strengthen the security of IT used by California schools against cyberattacks by permitting an LEA to request that the Military Department conduct an ISA of the agency or a schoolsite within its jurisdiction. This bill is author sponsored.

**2) Author's statement**: 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.
>
> Eventually the pandemic will end and schools will return to regular in-class learning. Yet still, schools have invested in remote technology to improve their students' educational experiences, and will continue to do so. […] 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. The department would share the assessments only with the LEAs at issue.

3) **Cybersecurity and schools**: As society's everyday reliance on technology grows, so too do the vulnerabilities to and costs associated with cybercrime. The Federal Bureau of Investigation's Internet Crime Complaint Center (FBI IC3) reported over two million complaints of internet crime over the past five years, totaling over $13 billion dollars in resulting losses. The number of reported internet crimes has increased every year since 2016, as have the associated costs, and the margin by which these rates increase year-over-year continues to grow. Between 2019 and 2020 alone, the number of complaints received by the FBI IC3 increased by nearly 70%, from 467,361 in 2019 to 791,790 in 2020, likely as a result of unprecedented demand for virtual technologies resulting from the COVID-19 pandemic. According to the FBI IC3's 2020 report, California leads the nation in both the number of complaints relating to internet crime, and in the estimated costs experienced by the victims. In 2020, the FBI IC3 received 69,541 cybercrime complaints from Californians, costing victims over $620 million – over $200 million more than New York, the next closest state.[1]

   The burden of this alarming increase in cybercrime has not been experienced equally across sectors. In particular, the education sector has been disproportionately subject to its effects. An ongoing analysis by Microsoft Security Intelligence indicates that over the last 30 days (as of March 28, 2021), the education sector has experienced over 63% of all enterprise malware encounters worldwide, amounting to nearly 7 million devices. The next closest sector, the business and professional services sector, accounts for only 9% of detected malware encounters, and just over 1 million devices.[2]

   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. A 2020 New York Times article described the issue as follows:

   > The coronavirus, which can spread easily when people gather closely indoors, thrust students and educators into remote learning with little time to prepare.

---

[1] Internet Crime Complaint Center, "Internet Crime Report 2020," *Federal Bureau of Investigation*, March 2021, https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics, [as of Mar. 28, 2021].
[2] Microsoft Security Intelligence, "Global threat activity: Most affected industries," *Microsoft*, https://www.microsoft.com/en-us/wdsi/threats, [as of Mar. 28, 2021].

> The digital infrastructure that makes remote learning possible is now increasingly seen as a target for cyberattacks. Schools are storing more data online without sophisticated plans for safeguarding it, and are susceptible to public pressure when that data is compromised, said Reuven Aronashvili, the founder and chief executive at CYE, a cybersecurity firm.
>
> Local governments, and schools in particular, are "considered to be quite low in cybersecurity maturity level," Mr. Aronashvili said in an interview.[3]

In other words, schools were already increasing their use of technology before the pandemic necessitated online learning, but because of strapped budgets, schools often do not appropriately invest in basic cybersecurity protections to accompany such technology. Schools are also more likely than other potential targets to have invested in insurance policies that will pay out in the event of ransomware attacks, making them more capable of paying ransoms that can cost tens or hundreds of thousands of dollars, and thus more attractive to malicious actors.[4]

These elevated cybersecurity risks are reflected in data demonstrating an unprecedented increase in publicly reported cyber incidents at schools over the course of the 2020 calendar year. As the K-12 Cybersecurity Resource Center's report "The State of K-12 Cybersecurity: 2020 Year in Review" lays out:

> Notwithstanding the heroic education IT-related efforts to ensure remote learning was possible for large numbers of elementary and secondary students and their teachers during 2020, it should hardly be surprising that school district responses to the COVID-19 pandemic also revealed significant gaps and critical failures in the resiliency and security of the K-12 educational technology ecosystem.
>
> Indeed, the 2020 calendar year saw a record-breaking number of publicly-disclosed school cyber incidents. Moreover, many of these incidents were significant: resulting in school closures, millions of [] stolen taxpayer dollars, and student data breaches directly linked to identity theft and credit fraud.

That report noted 408 publicly-disclosed school cyber incidents during the 2020 calendar year, including student and staff data breaches, ransomware and other malware outbreaks, phishing attacks and other social engineering scams, denial-of-service attacks, and "a wide variety of other incidents." This represents an 18% increase over the previous year's total, which had itself represented a nearly threefold increase over 2018, and amounts to an average of roughly two publicly-disclosed cyber incidents per school day.[5]

---

[3] Azi Paybarah, "Ransomware Attack Closes Baltimore County Public Schools," *The New York Times*, Nov. 29, 2020, https://www.nytimes.com/2020/11/29/us/baltimore-schools-cyberattack.html, [as of Mar. 27, 2021].
[4] Joseph Marks & Tonya Riley, "The Cybersecurity 202: Spiking ransomware attacks against schools make pandemic education even harder," *The Washington Post*, Dec. 11, 2020, https://www.washingtonpost.com/politics/2020/12/11/cybersecurity-202-spiking-ransomware-attacks-against-schools-make-pandemic-education-even-harder/, [as of Mar. 27, 2021].
[5] Douglas A. Levin, "The State of K-12 Cybersecurity: 2020 Year in Review," *K-12 Cybersecurity Resource Center*, Mar. 10, 2021.

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. The federal Family Educational Rights and Privacy Act (FERPA) provides parents and eligible students with the right to inspect and review the student's education records, and to request corrections to records they believe to be inaccurate, but generally prohibits disclosure of the student's education record without the consent of the parent or student, except under specified conditions. (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99.) California law similarly considers pupil records worthy of additional protection, and specifies several conditions and limitations on the use, maintenance, and disclosure of pupil records, including prohibiting a school district from permitting access to pupil records to a person without written parental consent or a lawfully issued subpoena or court order to do so. (Ed. Code Sec. 49073, et seq.) But these comprehensive privacy laws do not appear to protect such sensitive records against unauthorized access to and disclosure of student records that can result from a breach of cybersecurity.

This bill would provide an avenue by which LEAs can identify and address cybersecurity vulnerabilities in order to further protect these sensitive records and maintain the IT capabilities necessary to accomplish their educational mission.

4) **Independent Security Assessments (ISAs)**: 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 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, Ch. 768, Stats. 2018). In 2018, the Legislature passed AB 3075 (Berman, Ch. 241, Stats. 2018) which created the Office of Elections Cybersecurity within the Secretary of State, tasked with the primary mission to coordinate efforts between the Secretary of State and local elections officials to reduce the likelihood and severity of cyber incidents that could interfere with the security or integrity of elections. The Budget Act of 2020 (AB 89, Ting, Ch. 7, Stats. 2020) also made substantial investments in cybersecurity, including by allocating $11.1 million to various departments to enhance the cybersecurity of the State's critical infrastructure, and $2.9 million to protect patient health records by strengthening cybersecurity throughout the State's public health infrastructure.

Of relevance to this bill, in 2010, the Legislature passed AB 2408 (Smyth, Ch. 404, Stats. 2010), which, among other things, required the chief of 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. (Gov. Code Sec. 11549.3(a).) AB 2408 provided that all state entities shall implement the policies and procedures issued by OIS, including compliance with the information security and privacy policies, standards, and procedures issued by OIS, and with filing and incident notification requirements. (Gov. Code Sec. 11549.3(b).) Five years later,

the Legislature expanded on the authority of OIS by passing AB 670 (Irwin, Ch. 518, Stats. 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. (Gov. Code Sec. 11549.3(c)(1) and (2).) 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 3rd 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.

5) **AB 1352 would permit, but not require, LEAs to request ISAs**: 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. 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.

6) **Related legislation**: AB 809 (Irwin) would require 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 would require those agencies to perform a comprehensive ISA every two years for which they may contract with the Military Department.

   SB 767 (Becker) would establish the Digital Education Equity Program, which would provide a regionalized network for technical assistance to schools and school districts on the implementation of educational technology, as set forth in policies of the State Board of Education.

7) **Prior legislation**: AB 89 (Ting, Ch. 7, Stats. 2020) *See* Comment 4.

   AB 2669 (Irwin, 2020) was substantially similar to AB 809 (*see* Comment 6). This bill was not set for hearing in the Assembly Privacy and Consumer Protection Committee.

   AB 2813 (Irwin, Ch. 768, Stats. 2018) *See* Comment 4.

   AB 3075 (Berman, Ch. 241, Stats. 2018) *See* Comment 4.

   AB 3193 (Chau, 2018) would have required all state agencies, including those not under the direct authority of the governor, to comply with the information security and privacy standards and practices established by OIS, and to undergo ISAs as required by OIS. This bill died in the Senate Governmental Organization Committee.

   AB 670 (Irwin, Ch. 518, Stats. 2015) *See* Comment 4.

   AB 1172 (Chau, 2015) would have continued the existence of the California Cyber Security Task Force created by Governor Brown within the Office of Emergency Services until 2020, to act in an advisory capacity and make policy recommendations on cybersecurity for the state, and would have created a State Director of Cyber Security position with specified duties within the Office of Emergency Services. This bill died on the Senate Inactive File.

   AB 2408 (Smyth, Ch. 404, Stats. 2010) *See* Comment 4.

8) **Double referral**: This bill has been double referred to the Committee on Military and Veterans Affairs.

**REGISTERED SUPPORT / OPPOSITION**:

**Support**

None on file

**Opposition**

None on file

**Analysis Prepared by**: Landon Klein / P. & C.P. / (916) 319-2200