SENATE COMMITTEE ON MILITARY AND VETERANS AFFAIRS
Senator Bob Archuleta, Chair
2021 - 2022 Regular

Bill No:	AB 1352	**Hearing Date:**	6/30/21
Author:	Chau		
Version:	3/22/21 Amended		
Urgency:	No	**Fiscal:**	Yes
Consultant:	V Badillo		

Subject: Independent information security assessments: Military Department: local educational agencies

DESCRIPTION

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.

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 §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 §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 §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 §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 §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 §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 §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 §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 §49073, et seq.)

This bill:

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.

BACKGROUND

According to the Assembly Committee on Privacy and Consumer Protection:

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 June 21, 2021), the education sector has experienced over 63.54% 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]

Independent Security Assessments (ISAs). According to the Independent Security Assessment Notification Guide, an 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 Cyber Network Defense (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].

In 2015, the Legislature expanded on the authority of OIS by passing AB 670 (Irwin, Ch. 518, Stats. 2015), which authorized OIS to conduct 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 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."

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,

---

[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 Jun 21, 2021].

[2] Microsoft Security Intelligence, "Global threat activity: Most affected industries," Microsoft, https://www.microsoft.com/en-us/wdsi/threats, [as of Jun 21, 2021].

for-profit third-party services that may themselves fail to meet the stringent cybersecurity standards the State maintains for its own networks.

Military Department Resources. Currently the Military Department's CND performs virtually all ISAs of state agencies. As required by AB 670 (Irwin, Ch. 518, Stats. 2015) no fewer than 35 ISAs must be conducted on State Agencies annually. While CND is the default vendor for ISAs, there is a CDT procedure for a State Agency to request a third-party vendor conduct the ISA in lieu of CND, but this procedure is rarely exercised, and the State Agency must certify that the third-party vendor will assess the same standards as CND. Through planning and coordination with the California Department of Technology (CDT), CND has been able to schedule and conduct an ISA on every State Agency on a bi-annual cycle with its current staffing levels.

An ISA takes a considerable amount of time, and can take weeks depending upon the size, complexity, and preparedness of the State Agency. While an ISA is being conducted 2-6 CND members are onsite at the State Agency, conducting risk analysis and penetration testing. When the CND concludes their onsite assessment, a report is compiled and is presented to the State Agency, identifying vulnerabilities and giving recommendations on how to remediate both high and low risk threats.

CMD noted in its 2019 Leadership Accountability Report:

> The Cyber Team's staff salaries, equipment, and other operating costs are solely funded by the costs it charges agencies for the assessments. This is a risk that creates a hardship for the Military because it does not receive payments from agencies until two to three months after services are rendered. The Military must bear the Cyber Team's operating costs and must use its own budget intended for critical programs until payments are received. There is a risk that payments received may not meet the Cyber Team's budget requirements and expenses. The Cyber Team may not be able to provide the cyber vulnerability assessment due to insufficient payments. This could result in the State Chief Information Officer not complying with Government Code 11549.3 and state agencies not complying with SAM 5330.1.

CMD went on to identify multiple actions it would take to mitigate this risk, including "Request a shift of the Cyber Network Defense Team program from a cost recovery model to a funded cost model."

Unfortunately to date, a shift from a cost recovery model to a funded cost model has not occurred for the CND's ISA program. The Governor's Proposed 2021-22 Budget does include a BCP from CDT to shift the Office of Information Security's Information Security Program Audit (ISPA) from a cost recovery model to a funded cost model, however this is a distinct program and function of CDT that should not be confused with ISAs.

While ISAs take a considerable portion of CND's time, they are also tasked with jointly operating the California Cybersecurity Integration Center (Cal-CSIC). In the 2020-2021 State Budget an additional 8 staff positions were funded by a three year limited term General Fund allocation to CMD to continue conducting its activities at the Cal-CSIC. Before last year the Cal-CSIC was funded entirely through the federal government's Homeland Security Grant Program. The limited term budget action provided funding

short-term funding stability for CMD and the other state departments operating the Cal-CSIC (OES, CDT, CHP).

[This bill is triple referred to Senate Committees on Military & Veterans Affairs, Judiciary, and Education.]

COMMENT

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. Yet, perhaps the entities that have experienced this shift more dramatically than any others are California's LEAs, with schools being 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. 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. As California's schools become more reliant on computer systems, their need to effectively identify cybersecurity shortcomings will only heighten."

"AB 1352 would authorize the state's Military Department to work alongside LEAs in identifying and addressing any outstanding cybersecurity threats. More specifically, this bill would authorize the California Military Department to perform an independent security assessment at the request of, and in consultation with, a local educational agency (LEA) that is interested in having an assessment done."

Related/Previous Legislation. AB 809 (Irwin, 2021) 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. *Held in Assembly Committee on Appropriations.*

SB 767 (Becker, 2021) 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. *Currently in the Assembly Committee on Education.*

AB 89 (Ting, Ch. 7, Stats. 2020). A budget bill, it included 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.

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

AB 2813 (Irwin, Ch. 768, Stats. 2018) codified the California Cybersecurity Integration Center (Cal-CSIC).

AB 3075 (Berman, Ch. 241, Stats. 2018) created the Office of Elections Cybersecurity within the Secretary of State.

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) 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 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) 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

POSITIONS

Sponsor: Author.

Support: California IT in Education

Oppose: None on file.

-- END --