Date of Hearing: April 27, 2021

ASSEMBLY COMMITTEE ON MILITARY AND VETERANS AFFAIRS
Jacqui Irwin, 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: This bill has not been analyzed in a fiscal committee.

COMMENTS:

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."

The Assembly Committee on Privacy and Consumer Protection has prepared a substantial analysis on the growing exposure of schools to internet crime and digital security threats. Here, it suffices to note that schools and local educational agencies (LEAs) already lacked resources and sophistication to keep up with attackers, and that the rapid increase in schools' reliance on technology occasioned by the COVID-19 pandemic has only worsened that vulnerability.

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 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].

The prior analysis of this bill by the Privacy and Consumer Protection Committee thoroughly discussed the cybersecurity threats posed to LEAs and the need for cybersecurity resources including Independent Security Assessments (ISAs) to be made available to LEAs with their limited budgets and competing priorities that understandably focus on their core education function. This Committee must analyze whether the Military Department currently, or could with changes being contemplated to the State Budget, have the resources and capacity to entertain requests from LEAs without interfering with their core function of providing security to the State.

Military Department Resources

Currently the Military Department's Cyber Network Defense Team, sometimes referred to as the Cyber Team or "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.

The author may wish to consider the availability of CND to accept LEAs' request for ISA under this bill, with the current high demand and near exclusive scheduling for their services to State Agencies through CDT.

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 as 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.

The author may wish to consider the risk identified by CMD of the cost recovery model to the financial ability for CND to expand its ISA offerings including pre-hiring staff to increase availability, and the new risk of expanding a cost recovery model to LEAs who CMD may have similar or increased difficulties in receiving timely payments.

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).

The author may wish to consider the request for stable funding for the CND's participation at the Cal-CSIC, and the limited-term budget allocation secured, as demonstrating limited resources of CND which may be unwise to overcommit with additional duties?

Other Legislation Authorizing Use of CMD for ISAs

AB 809 (Irwin) of this year is similar to this bill in that it authorizes CMD to conduct ISAs on an additional group of public entities, certain State Agencies that do not report to the Governor (e.g. Constitutional Offices and Independent Boards) who currently under statute do not have to abide by state cybersecurity standards. If AB 809 were to become law, the potential customer base for

CND would be expanded even further than this bill contemplates. As these state-level entities may wish to use a fellow state department for their ISAs, this puts into question who CND should prioritize if requests from entities not required to use their services begin to outpace availability.

The author may wish to consider the potential to burden CND with the need to prioritize requests for its services, or if statute should more clearly define the priority for non-required ISA requests such as those from LEAs, Constitutional Offices, and Independent Boards.

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.

Prior legislation. 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

REGISTERED SUPPORT / OPPOSITION:

Support

California IT in Education.

Opposition

None on file.

Analysis Prepared by: Brandon Bjerke/Christian Burkin / M. & V.A. / (916) 319-3550