SENATE RULES COMMITTEE AB 1352
Office of Senate Floor Analyses
(916) 651-1520 Fax: (916) 327-4478

THIRD READING

Bill No: AB 1352
Author: Chau (D)
Amended: 8/24/21 in Senate
Vote: 21

SENATE MILITARY & VETERANS COMMITTEE: 6-0, 6/30/21
AYES: Archuleta, Grove, Eggman, Newman, Roth, Umberg
NO VOTE RECORDED: Melendez

SENATE JUDICIARY COMMITTEE: 11-0, 7/6/21
AYES: Umberg, Borgeas, Caballero, Durazo, Gonzalez, Hertzberg, Jones, Laird, Stern, Wieckowski, Wiener

SENATE APPROPRIATIONS COMMITTEE: Senate Rule 28.8

ASSEMBLY FLOOR: 76-0, 5/20/21 (Consent) - See last page for vote

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

SOURCE: Author

DIGEST: 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 Floor Amendments of 8/24/21 authorize the California Cybersecurity Integration Center to consult on LEA assessments and have access to assessment reports.

ANALYSIS:

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 (CPRA). (GOV §11549.3(f).)

7) Provides that nothing in CPRA 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) Authorizes the Military Department, at the request of a LEA, and in consultation with the California Cybersecurity Integration Center, to perform an in ISA of the LEA, or an individual schoolsite under its jurisdiction, the cost of which shall be funded by the LEA.

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

3) Specifies that the Military Department shall disclose the results of the ISA only to the LEA and the California Cybersecurity Integration Center.

Background

Cybersecurity and schools. 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.[1] 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

[1] Microsoft Security Intelligence, *Global Threat Activity,* https://www.microsoft.com/en-us/wdsi/threats, [as of Aug 16, 2021].

against kindergarten through grade 12 institutions, up from 28 percent in January through July 2020.[2] Schools often make 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.[3]

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. 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.[4]

Independent Security Assessments (ISAs). 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). 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. 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.

Additionally, this bill provides that the results of a Military Department independent security assessment will stay confidential, with two provisions. First,

---

[2] Marks, *The Cybersecurity 202: Spiking ransomware attacks against schools make pandemic education even harder*, Washington Post (Dec. 20, 2020), https://www.washingtonpost.com/politics/2020/12/11/cybersecurity-202-spiking-ransomware-attacks-against-schools-make-pandemic-education-even-harder/ [last visited Aug 16, 2021].
[3] *Ibid*.
[4] 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, [last visited Aug 16, 2021].

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. 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." 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; it therefore seems consistent to apply the same degree of confidentiality to the results of assessments performed for LEAs.

[NOTE: For further detail, please see the Senate Judiciary and/or Military & Veterans Affairs Committee analyses.]

FISCAL EFFECT: Appropriation: No Fiscal Com.: Yes Local: No

SUPPORT: (Verified 8/23/21)

California IT in Education

OPPOSITION: (Verified 8/23/21)

None received

ASSEMBLY FLOOR: 76-0, 5/20/21
AYES: 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
NO VOTE RECORDED: Cunningham, Kalra

Prepared by: V. Badillo / M.V.A. / (916) 651-1503
8/25/21 14:11:24

****** END ******