Date of Hearing: April 19, 2022

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
AB 2355 (Salas) – As Amended April 7, 2022

SUBJECT: School cybersecurity

SUMMARY: This bill would require local educational agencies (LEAs) to report cyberattacks impacting more than 500 pupils or personnel to the California Cybersecurity Integration Center (Cal-CSIC), and would require Cal-CSIC to track and annually report to the Legislature on cyberattacks and data breaches affecting LEAs. Specifically, **this bill would**:

1) Require an LEA, as defined, to report any cyberattack, as defined, impacting more than 500 pupils or personnel to Cal-CSIC.

2) Require Cal-CSIC to establish a database that tracks reports of cyberattacks submitted by LEAs pursuant to the bill.

3) Require that Cal-CSIC annually, by January 1, provide a report to the Governor and to the relevant policy committees of the Legislature summarizing the types and number of cyberattacks on LEAs, the types and number of data breaches affecting LEAs that have been reported to the Attorney General pursuant to existing data breach notification laws, any activities provided by Cal-CSIC to prevent cyberattacks or data breaches of an LEA, and support provided by Cal-CSIC following a cyberattack or data breach of an LEA.

4) Require that the Attorney General share sample copies of data breach notifications received from LEAs pursuant to existing data breach notification laws, excluding any personally identifiable information, with Cal-CSIC for the purpose of compiling the report required by 3), above.

5) Define "cyberattack," for the purposes of the bill, to mean either of the following: 1) any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by unauthorized access; or 2) the unauthorized denial of access to legitimate users of a computer system, computer network, computer program, or data.

6) Define "local educational agency," for the purposes of the bill, to mean a school district, county office of education, or charter school.

7) Specify that the provisions of the bill shall remain in effect only until January 1, 2027, and as of that date are repealed.

EXISTING LAW:

1) Establishes, within the office of the Governor, the Office of Emergency Services (CalOES), with responsibility for the state's emergency and disaster response services for natural, technological, or man-made disasters and emergencies, including responsibility for activities necessary to prevent, respond to, recover from, and mitigate the effects of emergencies and disasters to people and property. (Gov. Code Sec. 8585(a) and (e).)

2) Tasks CalOES with establishing and leading Cal-CSIC, comprised of representatives from specified state and federal agencies and offices, with the primary mission of reducing the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks in our state; and provides that Cal-CSIC shall serve as the central organizing hub of state government's cybersecurity activities and coordinate information sharing with local, state, and federal agencies, tribal governments, utilities and other service providers, academic institutions, and nongovernmental organizations. (Gov. Code Sec. 8586.5(a).)

3) Tasks Cal-CSIC with establishing a Cyber Incident Response Team to serve as California's primary unit to lead cyber threat detection, reporting, and response in coordination with public and private entities across the state. (Gov. Code Sec. 8586.5(d).)

4) Provides that information sharing by Cal-CSIC shall be conducted in a manner that protects the privacy and civil liberties of individuals, safeguards sensitive information, preserves business confidentiality, and enables public officials to detect, investigate, respond to, and prevent cyberattacks that threaten public health and safety, economic stability, and national security. (Gov. Code Sec. 8586.5(e).)

5) Requires any agency that owns or licenses computerized data that includes personal information (PI) to disclose a breach of the security of the system, as defined, to any California resident whose unencrypted PI, or encrypted PI along with an encryption key or security credential, was, or is reasonably believed to have been, *acquired* by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as specified. (Civ. Code Sec. 1798.29(a) and (c).)

6) Requires any person or business that owns or licenses computerized data that includes PI to disclose a breach of the security of the system to any California resident whose unencrypted PI, or encrypted PI along with an encryption key or security credential, was, or is reasonably believed to have been, *acquired* by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as specified. (Civ. Code Sec. 1798.82(a) and (c).)

7) Requires any agency, person, or business that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system pursuant to 5) or 6), above, to electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. (Civ. Code Secs. 1798.29(e) and 1798.82(f).)

8) Defines "agency," for the purposes of 5) and 7), above, to include a local agency; and further defines local agency, pursuant to subdivision (a) of Section 6252 of the Government Code, to include a county; city, whether general law or chartered; city and county; school district; municipal corporation; district; political subdivision; or any board, commission or agency thereof; other local public agency; or entities that are legislative bodies of a local agency, as specified. (Civ. Code Sec. 1798.29(k); Gov. Code Sec. 6252(a).)

9) Defines "breach of the security of the system," for purposes of the data breach notification statute, to mean unauthorized *acquisition* of computerized data that compromises the

security, confidentiality, or integrity of PI maintained by the agency, person, or business, and excludes from that definition the good faith acquisition of PI by an employee or agent of the agency, person, or business for the purposes of the agency, person, or business, provided that PI is not used or subject to further unauthorized disclosure. (Civ. Code Secs. 1798.29(f); 1798.82(g).)

10) 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.)

11) 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**: This bill seeks to address the rising prevalence of cyberattacks on schools by requiring LEAs to report the occurrence of major cyberattacks affecting their pupils and personnel to Cal-CSIC, requiring Cal-CSIC to track these events, and requiring Cal-CSIC to summarize the information gathered in annual reports to the Legislature to inform future policy. This bill is author sponsored.

2) **Author's statement**: According to the author:

> [T]he lack of reporting [on cyberattacks on schools] has meant that many California schools are either unaware or do not believe cyberattacks will impact their school. IBM surveyed 1,000 educators and 200 administrators from K-12 schools. The results show that many are not ready to deal with future cyberattacks, nor do they have much understanding regarding how common it is. Being aware of rising trends in cyberattacks allows for schools to make informed decisions and address the threat. The collection and tracking of data is crucial in combating cyberattacks and protecting the sensitive information of students and teachers.
>
> This bill will help ensure schools collect consistent data regarding cyberattacks to ensure further transparency and protection against breaches. There needs to be data and information to begin with so that the scope of attacks can be better understood. This will also equip researchers and schools with necessary and consistent information needed to adopt solutions to the problem.

3) **Cybersecurity and schools**: As society's reliance on technology grows, so do the vulnerabilities to and costs associated with cybercrime. The Federal Bureau of Investigation's Internet Crime Complaint Center (FBI IC3) reported nearly three million complaints of internet crime over the past five years, totaling almost $19 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 2021 report, California leads the nation by a staggering margin in both the number of victims of internet crime and in the estimated costs experienced by the victims, with nearly 50% more victims and over twice the costs compared to the next closest states, respectively.[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 April 10, 2022), the education sector has experienced roughly 83% of all enterprise malware encounters worldwide, amounting to over 7.2 million devices. The next closest sector, the retail and consumer goods sector, accounts for only 8% of detected malware encounters, and just over 700,000 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 was essential to facilitate the remote learning environment necessitated by efforts to combat the pandemic. 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.[3]

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. Though a 2022 Annual Report surveying cyber incidents at K-12 schools during the 2021 calendar year indicated a marked decrease from the 2020 figures, the author of the report implicates outstanding deficiencies in public reporting of cyber incidents as responsible for the decrease, suggesting that these numbers may not accurately reflect the true state of school cybersecurity:

> [B]y and large, public-disclosure requirements for school districts and their vendors are quite weak. […] The lack of more robust K-12 cyber incident public disclosure requirements only serves to obscure the realities of school district and vendor operations

---

[1] Internet Crime Complaint Center, "Internet Crime Report 2021," *Federal Bureau of Investigation*, Mar. 22 2022, https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2021-internet-crime-report, [as of Apr. 9, 2022].
[2] Microsoft Security Intelligence, "Global threat activity: Most affected industries," *Microsoft*, https://www.microsoft.com/en-us/wdsi/threats, [as of Apr. 10, 2022].
[3] 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].

> from those charged with oversight, and to place school community members at unnecessary risk. As such, the smaller number of incidents reported during 2021 may instead reflect a concerning shift away from public disclosure, undermining the ability of independent researchers – and the policymakers and school system leaders who rely on their work – to accurately assess trends and issues.[4]

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, or denial of necessary access to, highly sensitive pupil records. This bill would provide a mechanism by which schools would be required to report major cyberattacks to Cal-CSIC in order to improve public accounting of these events and better inform policy and practices moving forward.

4) **Reporting of data breaches under existing law**: In 2002, this Legislature passed AB 700 (Simitian, Ch. 1054, Stats. 2002) and SB 1386 (Peace, Ch. 915, Stats. 2002) which created the Data Breach Notification Law (DBNL) to require a state agency, person, or business that conducts business in California, that owns or licenses computerized data including PI, to disclose any breach of the security of that data to California residents whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person. The DBNL is divided into two independent code sections within the Civil Code, one of which applies to information held by persons or businesses (i.e. private entities; Civ. Code Sec. 1798.82), and the other of which is located within the Information Practices Act of 1977 (IPA) and applies to information held by public agencies. (Civ. Code Sec. 1798.29.)

   Both the public and private DBNLs provide detailed specifications concerning required notifications disclosing when an agency, person, or business that owns or licenses computerized data that includes PI has suffered a "breach of the security of the system," and define "breach of the security of the system" to mean "unauthorized *acquisition* of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency." (Civ. Code Secs. 1798.29(f) and 1798.82(g); emphasis added.) In the event of such a breach, the DBNLs require that the breach be disclosed to any resident whose PI was, or is reasonably believed to have been, acquired by an unauthorized person (Civ. Code Secs. 1798.29(a) and 1798.82(a)), and, if the agency, person, or business is required to issue a breach notification to more than 500 California residents as a result of a single breach, they must also submit a sample copy of the breach notification to the Attorney General. (Civ. Code Secs. 1798.29(e) and 1798.82(f).)

   Data breaches vs. other cyberattacks: Notably, these disclosure and notification requirements apply only in the event that data containing PI are *acquired* without authorization. However, data breaches, i.e. attacks characterized by unauthorized acquisition of PI, are only one of a number of possible cyberattacks that could affect an LEA, including ransomware, denial-of-service, business email compromise scams, and website and social media defacement. These types of cyberattacks do not by definition require any PI to be compromised, but nonetheless substantially impede the educational mission of LEAs. According to the 2022 Annual Report on "State of K-12 Cybersecurity,"[5] less than one third

---

[4] Douglas A. Levin, "The State of K-12 Cybersecurity: Year in Review – 2022 Annual Report," *K-12 Security Information Exchange (K12 SIX)*, Mar. 2022.
[5] *Id.* at p. 7.

of all publicly disclosed cyber incidents involved data breaches, with ransomware attacks, in which the assailant precludes access to essential computer systems unless a ransom is paid, being most frequent. Because these attacks fall outside of the definition of "breach of the security of the system," the existing mechanism for ensuring public accounting of major incidents, i.e. disclosure of data breaches affecting over 500 individuals to the Attorney General, arguably does not apply, resulting in a dearth of reliable information about the prevalence and nature of cyberattacks affecting LEAs that could inform policy and practices.

LEAs and data breach notification laws: While the IPA generally exempts local agencies from its requirements, in 2013, this Legislature passed AB 1149 (Campos, Ch. 395, Stats. 2013), which, among other things, explicitly applied the DBNL provisions of the IPA to local agencies, stating that "[n]otwithstanding the exception specified in paragraph (4) of subdivision (b) of Section 1798.3, for purposes of this section, 'agency' includes a local agency, as defined in subdivision (a) of Section 6252 of the Government Code." (Civ. Code Sec. 1798.29(k).) Since that time, California has added numerous provisions to the DBNL to protect residents as data breaches become more commonplace. For example, AB 2828 (Chau, Ch. 337, Stats. 2016) required notification of breaches of encrypted PI if an encryption key or security credential that could render the PI readable was also compromised in the breach, AB 1130 (Levine, Ch. 750, Stats. 2019) added government-issued identification numbers and unique biometric data to the DBNL definition of PI, and AB 825 (Levine, Ch. 527, Stats. 2021) further included genetic data. Nonetheless, the provision applying the DBNL to local agencies has remained unchanged.

Despite the explicit inclusion of local agencies in the DBNL, it is not entirely clear how the DBNL applies to LEAs as they are defined in this bill. Subdivision (k) of Section 1798.29 of the Civil Code, which applies the DBNL to local agencies, cross-references a definition of "local agency" from the California Public Records Act which defines it to include "a county; city, whether general law or chartered; city and county; *school district*; municipal corporation; district; political subdivision; *or any board, commission or agency thereof*; *other local public agency*; or entities that are legislative bodies of a local agency pursuant to subdivisions (c) and (d) of Section 54952." (Gov. Code Sec. 6252 (a).) This bill defines LEA to include a school district, county office of education, or charter school. While the definition of "local agency" used in the DBNL expressly includes school districts, neither county offices of education nor charter schools are included by name. Arguably, county offices of education would be captured by this definition, as they would either be considered a "board, commission or agency" of a county, or an "other local public agency."

Whether the definition includes charter schools, however, is unclear. Charter schools are generally authorized by school districts or county offices of education, and thus could conceivably be considered agencies of their authorizing district/county office, but they also operate independently from that school district or county office and are not bound by many of the regulations governing public school systems. Definitions of "local educational agency," which nominally implies characteristics that may qualify an entity as an "other local public agency," vary in whether or not they include charter schools. Pursuant to Section 47604.1 of the Education Code, charter schools are subject to several laws governing the operations of local agencies, including the Ralph M. Brown Act ((b)(1)), the Political Reform Act of 1974 ((b)(4)), and, of particular note, the California Public Records Act ((b)(2)). One possible interpretation of the express application of the Public Records Act to charter schools in the Education Code is that charter schools may, absent that provision, otherwise be

interpreted to fall outside of the Act. This would mean the definition of "local agency" within the Public Records Act, which is cross-referenced in the public DBNL, does not include charter schools, and therefore would imply that charter schools are not bound by the DBNL provisions within the IPA. The DBNL outside of the IPA that applies to a "person or business that conducts business in California" may still apply, however, and contains substantially similar notification and disclosure requirements to the DBNL governing local agencies.

5) **AB 2355 would require cyberattacks impacting LEAs to be reported to Cal-CSIC**: This bill seeks to complement existing DBNLs by requiring more consistent accounting of cyber incidents other than data breaches that impact LEAs. Specifically, the bill would do all of the following:

   - Require an LEA to report any cyberattack impacting more than 500 pupils or personnel to Cal-CSIC.
   - Require Cal-CSIC to establish a database that tracks cyberattacks submitted by LEAs pursuant to the previous provision.
   - Require Cal-CSIC to annually provide a report to the Governor and the relevant policy committees of the Legislature summarizing the types and number of cyberattacks on LEAs, the types and number of data breaches affecting LEAs that have been reported to the Attorney General pursuant to the existing public DBNL, any activities provided by Cal-CSIC to prevent cyberattacks or data breaches of an LEA, and support provided by Cal-CSIC following a cyberattack or data breach of an LEA.
   - Require the Attorney General to share sample copies of data breach notifications received from LEAs pursuant to the existing public DBNL, excluding any personally identifiable information, with Cal-CSIC for the purpose of compiling the report pursuant to the previous provision.
   - Specify that the provisions of the bill shall only remain in effect until January 1, 2027.
   - Define, for the purposes of the bill, "California Cybersecurity Integration Center" or "Center," "cyberattack," and "local educational agency".

   The bill defines "cyberattack" to mean either of the following: 1) any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by unauthorized access; or 2) the unauthorized denial of access to legitimate users of a computer system, computer network, computer program, or data. This definition, while fairly expansive in order to cover the diverse tactics through which information technology can be disrupted, seems to prudently exclude data breaches, as it does not refer to the *acquisition* of data resulting from unauthorized access. Because disclosure of data breaches is already governed by existing laws (*see* Comment 4), defining "cyberattack" to include data breaches would risk enacting confusing and redundant notification requirements. Accordingly, the definition of "cyberattack" used in this bill seems appropriately inclusive as

to ensure that the state receives some accounting of major cyber incidents without overlapping existing law.

AB 2355 limits required reporting by LEAs to cyberattacks that "[impact] more than 500 pupils or personnel," but the bill does not specify what constitutes "impacting" a pupil or personnel. The threshold of 500 individuals is clearly intended to parallel the similar provision in the DBNL requiring an agency, person, or business that is required to issue a security breach notification to more than 500 California residents to submit a sample of the breach notification to the Attorney General. (Civ. Code. Secs. 1798.29(g) and 1798.82(f).) In that case, however, the number of impacted individuals is far easier to ascertain, since those events concern the compromise PI, which is, by definition, associated with individuals.

In contrast, cyberattacks subject to this bill are not necessarily delineated by the number of affected parties. If, for instance, a school of 800 students falls victim to a ransomware attack that temporarily shuts down the school's computer system but does not require the school to close, it is not clear how to determine the number of pupils and personnel affected. Would impacted parties be only those who needed to access the computer system during that time? Or would it include anyone whose PI was contained on that system? Similarly, if the school's website is hacked and defaced with lewd images, would the number of pupils and personnel affected be limited to those who viewed the hacked website before it was remediated?

The lack of clarity in determining impacted parties has the potential to result in inconsistent reporting by LEAs depending on the nature of the attack and the LEA's interpretation of the requirement, undermining the value of the accounting the bill attempts to establish. Accordingly, as this bill moves through the legislative process, the author may wish to consider defining what constitutes an impacted pupil or personnel, or substituting a clearer threshold for evaluating whether a major cyberattack requires disclosure.

Despite this shortcoming, the disclosure and reporting requirements in this bill arguably provide necessary insight into the cybersecurity status of California's educational institutions at a time when cyberattacks on schools are increasingly common. The information gleaned from this reporting, and the establishment of the requisite database at Cal-CSIC, has the potential to inform best practices undertaken by schools to mitigate cyber incidents and to identify policies for consideration by this Legislature to protect the integrity of the state's educational infrastructure.

6) **Author's amendments**: The author of this bill took several amendments in the previous policy committee to ensure that the provisions of this bill could work in tandem with existing DBNLs to provide for comprehensive accounting of major cyber incidents affecting LEAs without complicating compliance. Toward this same end, the author has agreed to two additional amendments to clarify the relationship between this statute and the existing DBNLs and to ensure that reports concerning cyber incidents affecting LEAs include all relevant occurrences.

Amendment 1: As discussed in Comment 5, the definition of "cyberattack" was thoughtfully crafted to avoid redundancy with the DBNL, but given the similarity between the two statutes, it is possible that an LEA could interpret the existence of this law to imply that they are subject only to the disclosure requirements under this bill and are not subject to those in the DBNL, particularly since the two statutes would reside in different codes altogether (i.e.,

Education Code vs. Civil Code). To clarify that this is not the case, the author has agreed to the following amendment, which explicitly indicates that compliance with both the DBNL and this bill would be required, as applicable:

Author's amendment:

On page 3, after line 31, insert: "***(c) Nothing in this section shall be construed to affect any disclosure or notification requirements pursuant to Sections 1798.29 and 1798.82 of the Civil Code.***"

Amendment 2: As discussed in Comment 4, it is not entirely clear whether charter schools, which are included in this bill's definition of "local educational agency," are subject to the DBNL pertaining to public agencies (i.e., Civ. Code Sec. 1798.29) or to the DBNL pertaining to persons and businesses (i.e., Civ. Code Sec. 1798.82). If charter schools are in fact subject to the DBNL pertaining to persons and businesses rather than the law for public agencies, the bill in print would not allow for transmission of sample data breach notices from the Attorney General to Cal-CSIC pertaining to major breaches of charter schools, and the ensuing report to the Legislature would consequently exclude that information. The result would be a report that does not adequately represent the full scope of major cyber incidents affecting LEAs as contemplated by the bill. To allow for the possible interpretation that charter schools are subject to the DBNL for persons and businesses rather than the DBNL for public agencies, the author has agreed to the following amendment:

Author's amendment:

On page 3, line 22, strike out "Section 1798.29" and insert: "***Sections 1798.29 and 1798.82***".

On page 3, line 29, strike out "Section 1798.29" and insert: "***Sections 1798.29 and 1798.82***".

1) **Related legislation**: AB 1711 (Seyarto) would require a person or business operating an information system on behalf of an agency that is required to disclose a breach of that system pursuant to existing law, to also disclose the breach by conspicuously posting the requisite notice on the agency's website, if the agency maintains one.

   AB 2135 (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 independent security assessment (ISA) every two years for which they may contract with the Military Department or a qualified responsible vendor.

   AB 2190 (Irwin) would enact a recommendation from the State Auditor's 2022 report (*see* Comment 7) to require that the Department of Technology confidentially submit an annual statewide information security status report, including specified information, to the Chair of the Assembly Committee on Privacy & Consumer Protection no later than January 2023.

   Prior legislation: AB 825 (Levine, Ch. 527, Stats. 2021) *See* Comment 4.

AB 1352 (Chau, Ch. 593, Stats. 2021) *See* Comment 3.

AB 2326 (Salas, 2020) would have required an LEA to report any cyberattack to Cal-CSIC and to designate a cybersecurity coordinator to serve as a liaison in cybersecurity matters between the LEA and Cal-CSIC. The bill would have further required Cal-CSIC to establish a database that tracks reports of cyberattacks submitted by LEAs and required Cal-CSIC to annually report to the Legislature on the state of cybersecurity in the state's LEAs. This bill was held in the Assembly Committee on Education.

AB 3276 (Chau, 2020) would have expressed the intent of the Legislature to enact subsequent legislation that would require every school district in the state to conduct an IT cybersecurity assessment. This bill died at the Assembly Desk.

AB 1130 (Levine, Ch. 750, Stats. 2019) *See* Comment 4.

AB 2813 (Irwin, Ch. 768, Stats. 2018) required the Office of Emergency Services (Cal OES) 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.

AB 3075 (Berman, Ch. 241, Stats. 2018) 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.

AB 2828 (Chau, Ch. 337, Stats. 2016) *See* Comment 4.

AB 1172 (Chau, 2015) would have continued the existence of the California Cyber Security Task Force created by Governor Brown within Cal OES 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 Cal OES. This bill died on the Senate Inactive File.

AB 1149 (Campos, Ch. 395, Stats. 2013) *See* Comment 4.

AB 700 (Simitian, Ch. 1054, Stats. 2002) *See* Comment 4.

SB 1386 (Peace, Ch. 915, Stats. 2002) *See* Comment 4.

7) **Double-referral**: This bill was double-referred to the Assembly Committee on Education where it was heard on April 6, 2022 and passed out 7-0.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

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