Date of Hearing: April 26, 2023

ASSEMBLY COMMITTEE ON EDUCATION
Al Muratsuchi, Chair
AB 1023 (Papan) – As Amended March 23, 2023

[Note: This bill is double referred to the Assembly Emergency Management Committee and was heard by that Committee as it relates to issues under its jurisdiction.]

SUBJECT: California Cybersecurity Integration Center: school cybersecurity

SUMMARY: Requires the California Cybersecurity Integration Center (Cal-CSIC) to 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, nongovernmental organizations, and academic institutions, including school districts, county offices of education (COEs), and charter schools. Specifically, **this bill**:

1) Requires the Cal-CSIC to 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, nongovernmental organizations, and academic institutions, including school districts, COEs, and charter schools.

2) Requires the Cal-CSIC to be composed of representatives from the following organizations:

    a) The Office of Emergency Services (Cal OES);

    b) The Office of Information Security;

    c) The State Threat Assessment Center;

    d) The Department of the California Highway Patrol;

    e) The Military Department;

    f) The Office of the Attorney General;

    g) The California Health and Human Services Agency;

    h) The California Utilities Emergency Association;

    i) The California State University;

    j) The University of California;

    k) The California Community Colleges;

    l) The California Department of Education (CDE);

    m) The United States Department of Homeland Security;

n) The United States Federal Bureau of Investigation (FBI);

o) The United States Secret Service;

p) The United States Coast Guard; and

q) Other members as designated by the Director of Emergency Services.

3) Requires the Cal-CSIC to operate in close coordination with the California State Threat Assessment System and the United States Department of Homeland Security — National Cybersecurity and Communications Integration Center, including sharing cyber threat information that is received from utilities, academic institutions, including school districts, COEs, and charter schools, private companies, and other appropriate sources. Requires the Cal-CSIC to provide warnings of cyberattacks to government agencies and nongovernmental partners, coordinate information sharing among these entities, assess risks to critical infrastructure and information technology networks, prioritize cyber threats and support public and private sector partners in protecting their vulnerable infrastructure and information technology networks, enable cross-sector coordination and sharing of recommended best practices and security measures, and support cybersecurity assessments, audits, and accountability programs that are required by state law to protect the information technology networks of California's agencies and departments.

EXISTING LAW:

1) Establishes, within the Government Operations Agency, the Department of Technology (DOT), 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. (Government Code (GC) 11545, et seq.)

2) Establishes, within the DOT, 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. (GC 11549(a) and (c))

3) Requires the chief of the 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. (GC 11549.3(a))

4) Authorizes the OIS to conduct, or require to be conducted, an Independent Security Assessment (ISA) of every state agency, department, or office, and requires the cost of the ISA to be funded by the state agency, department, or office being assessed, and specifies that OIS must, in consultation with the Cal OES, annually require no fewer than 35 state entities to perform an ISA. (GC 11549.3(c)(1) and (2))

5) Authorizes the Military Department to perform an ISA of any state agency, department, or office, and requires the cost of the ISA to be funded by the agency, department, or office being assessed. (GC 11549.3(c)(3))

6) Authorizes the Military Department to perform an ISA of an LEA defined as a school district, COE, charter school, or state special school. (GC 11549.3(i))

7) Requires that, notwithstanding any other law, during the process of conducting an ISA, information and records concerning the ISA are confidential and 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 (PRA). (GC 11549.3(f))

8) Requires that nothing in the California PRA 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. (GC 6254.19)

9) Authorizes a local educational agency (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. (Education Code (EC) 49073.1(a))

10) 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. (EC 49073)

11) Establishes the Cal-CSIC under the Cal OES. (GC 8586.5)

12) Requires the disclosure of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the agency that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable. (Civil Code (CC) 1798.29)

FISCAL EFFECT: Unknown

COMMENTS:

Need for the bill. According to the author, "The California Cybersecurity Integration Center coordinates information sharing at all levels of government agencies, utilities and other service providers, academic institutions, and nongovernmental organizations. With the rise of cyber threats, this group is imperative to protect sensitive, personal data in public and private networks

and databases. Unfortunately, our K-12 schools are not involved with this group, yet have recently been the target of cyberattacks. Our school districts maintain sensitive medical and financial data on staff and students and their families. AB 1023 will include LEAs in Cal-CSIC and allow them to become informed and prepared for cyber threats."

California Cybersecurity Integration Center (Cal-CSIC). According to the Cal OES, Cal-CSIC is a Cal OES division with the primary mission to "reduce 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." In 2018, the Governor signed AB 2813 (Chapter 768, Statutes of 2018) further defining the structure and mission of Cal-CSIC. Cal-CSIC is structured to have the following:

- A Cyber Incident Response Coordination Team to lead cyber threat detection, reporting, and response in coordination with public and private entities across the state. This team assists law enforcement agencies with primary jurisdiction for cyber-related criminal investigations and agencies responsible for advancing information security within state government;

- The Cal-CSIC serves as a conduit for cybersecurity threat information between federal, state, local, and tribal government entities. Advisories and Alerts are also shared with private sector partners;

- Provides the exchange of intelligence-driven cyber threat indicators between the Cal-CSIC cyber threat feeds and partner entities at machine speed, resulting in the distribution of relevant and timely cyber threat and trend information; and

- Cal-CSIC Analysts collect and analyze phishing emails to extrapolate relevant information about the attacker and their respective tactics, called Indicators of Compromise (IOC). These IOCs are added to the California Automated Indicator Exchange to ensure timely distribution to partner entities.

Increasing frequency of cyberattacks on LEAs. According to a 2021 article by CalMatters, *Under Attack: California Schools Face Ransomware Threat*, more than two dozen California school systems have been targets of cyberattacks. Since 2016, Seculore Solutions, a software company, has recorded over 122 cyberattacks in California across the public safety, government, medical, and education sectors with at least 26 cyberattacks targeting school districts and universities. In the 2021 CalMatters article, a UC Berkeley cybersecurity researcher stated, "If the data on cyberattacks seems sketchy and incomplete, that's because it is." With many schools adopting distance learning in the 2019-20 and 2020-21 school years, technological vulnerabilities increase yet little information is collected regarding the nature of the attacks, and the resulting impact on agencies.

A variety of LEAs, from a rural northern California COE to the Los Angeles Unified School District, have experienced significant cyberattacks in the last several years. Each attack is different, but may cause disruptions in e-mail access, financial software, and internet capabilities. Without internet access, LEAs operations come to a halt, and may disrupt activities such as administering standardized testing during a critical time of assessing students' academic progress. The security of confidential student and personnel records may also be threatened.

According to the FBI, ransomware is a type of malicious software, or malware, which prevents a user from accessing computer files, systems or networks and demands the user pay a ransom for their return. Once a user unknowingly downloads the ransomware onto a computer by, for example, opening an e-mail attachment, the malware is then loaded into the user's computer and locks access to data and files stored in the system. In some cases, the FBI works with the impacted LEA and their cybersecurity team to aid in the situation.

California Department of Education's cybersecurity response. The CDE collects and protects student data. To protect and maintain sensitive information and awareness throughout the year, the Educational Data Governance Program hosts presentations by cybersecurity and privacy experts from federal partner agencies such as the FBI and the U.S. Department of Education. Additionally, CDE staff network and learn from privacy professionals and share privacy resources with schools and districts at conferences and symposia. Schools are currently not required to report cyberattacks to the CDE.

Federal response to cyberattacks on K-12 education. In 2020, a joint cybersecurity advisory authored by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC), *Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data,* the advisory report documents the common types of attacks used by cybercriminals that can lead to theft of data and disruption of distance learning services, and a loss of basic school operational functions. The common attacks identified in the report are ransomware, malware, distributed denial-of-service attacks (DDoS), and video conference disruptions. The report suggests that "cyber actors likely view schools as targets of opportunity and that these types of attacks are expected to continue through the 2020-2021 academic year." These issues are particularly challenging for K-12 schools that face resource limitations; therefore, educational leadership, information technology personnel, and security personnel will need to balance this risk when determining their cybersecurity investments.

To mitigate these attacks, the FBI encourages education providers to review, update, and maintain best IT practices like patching plans, security policies, and user agreements. The report lists best practices for both school IT networks, in general, and tips on how to defend against the common attacks. The report also provides an example of code that has been used to detect and defend against related attacks. Finally, it offers a list of online resources that schools may use to help strengthen their cybersecurity system. The CISA started a campaign to bring attention to the recent increase in cyberattacks at schools and healthcare institutions. CISA's initiative, "Reduce the Risk of Ransomware Campaign," will include education by CISA through its website and social media pages on how entities can best protect themselves from attacks. CISA has also launched an online resource center that includes best practice guides for network administrators. Schools are particularly vulnerable to these attacks and risk the exposure of personal information of minors when facing a cyberattack.

Data breach reporting. According to the Attorney General (AG) of California, California law requires a business, state agency, or local agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person, and requires a breach notification to the AG when more than 500 California residents are believed to be impacted. "Local agency" includes 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. The eCrime Unit, a division in the Office of the AG, is tasked with investigating and prosecuting criminal organizations that commit identity theft crimes, use an electronic device or network to facilitate a crime, or commit a crime targeting an electronic device, network or intellectual property in excess of $50,000. Any agency or entity can voluntarily report data breaches to the AG. However, the data breach reports are only for notification purposes; the AG does not provide funding or services for affected entities.

COVID-19 impact on cybersecurity. According to a 2020 report by Interpol, *Cybercrime: COVID-19 impact*, the COVID-19 pandemic has severely affected the global cyber threat landscape. The sharp increase in cybercriminal activities related to COVID-19 has put significant strain on law enforcement communities worldwide. To maximize damage and financial gain, cybercriminals have shifted their targets from individuals to larger entities like major corporations, governments, and institutions. Due to the sudden shift to teleworking, organizations have had to rapidly deploy remote systems, networks, and applications resulting in increased security vulnerabilities to steal data, generate profits and cause disruption. The FBI's Internet Crime Complaint Center 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 Internet Crime Complaint Center 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 Internet Crime Complaint Center'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 Internet Crime Complaint Center received 69,541 cybercrime complaints from Californians, costing victims over $620 million – over $200 million more than New York, the next closest state.

Arguments in support. The California School Boards Association writes, "Currently, there are over 1,000 local education agencies (LEAs) in California representing almost 6 million students, over 500,000 staff and 10,000 school sites. Over the last few years, ransomware attacks on California's LEAs have increased. For many districts it is not a matter of if, but when they will be subject to a cybersecurity attack which can render the entire school district unable to conduct the business of educating students. By specifically including LEAs as an academic institution under Cal-CSIC, it will ensure that LEAs receive information and guidance to address issues of cybersecurity and protecting student data and privacy."

Related legislation. AB 2355 (Salas), Chapter 498, Statutes of 2022, requires an LEA to report a cyberattack impacting 500 or more pupils or personnel to report to the Cal-CSIC and requires the Cal-CSIC to annually report to the Governor and relevant policy committees of the Legislature with specified information related to the cyberattack.

AB 1352 (Chau), Chapter 593, Statutes of 2021, authorizes the Military Department, at the request of an LEA, and in consultation with the Cal-CSIC, to perform an independent security assessment of the LEA, or an individual schoolsite under its jurisdiction, the cost of which is to be funded by the LEA, as specified.

AB 2326 (Salas) of the 2019-20 Session would have required an LEA to report any cyberattack to the Cal-CSIC and to designate a cybersecurity coordinator to serve as a liaison in cybersecurity matters between the LEA and the Cal-CSIC. The bill would have required the Cal-CSIC to establish a database that tracks reports of cyberattacks submitted by LEAs and required the 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 Education Committee.

AB 3276 (Chau) of the 2019-20 Session 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 was held in the Rules Committee.

AB 1566 (Chau) of the 2019-20 Session would have established the California Cyber Range Pilot Project, under the administration of the Cal-CSIC, to test the overall feasibility of the pilot project through a yearlong effort. The bill would have required the pilot project to produce a scalable model for a permanent California Cyber Range Program. This bill was held in the Assembly Higher Education Committee.

AB 2564 (Chau) of the 2019-2020 Session would have stated the intent of the Legislature to enact legislation to improve the security of IT systems and connected devices by requiring public agencies and businesses to develop security vulnerability disclosure policies. This bill was held in the Rules Committee.

AB 2813 (Irwin), Chapter 768, Statutes of 2018, establishes the Cal-CSIC within the Cal OES, the primary mission of which is the same as Cal-CSIC as created by Executive order. The bill requires Cal-CSIC to include representatives from the Cal OES, the Office of Information Security, the State Threat Assessment Center, the Department of the California Highway Patrol, the Military Department, the Office of the AG, the California Health and Human Services Agency, and others. Required the Cal-CSIC to coordinate with the California State Threat Assessment System and the U.S. Department of Homeland Security, establish a cyber incident response team, and safeguard the privacy of individuals' sensitive information.

REGISTERED SUPPORT / OPPOSITION:

Support

California Federation of Teachers
California School Boards Association
Los Angeles Unified School District

Opposition

None on file

Analysis Prepared by: Marguerite Ries / ED. / (916) 319-2087