Date of Hearing: April 18, 2018

ASSEMBLY COMMITTEE ON GOVERNMENTAL ORGANIZATION
Adam Gray, Chair
AB 2813 (Irwin) – As Amended March 23, 2018

SUBJECT: California Cybersecurity Integration Center

SUMMARY: This bill would establish the California Cybersecurity Integration Center (Cal-CSIC), as specified, and require it to develop a cybersecurity strategy for California. Specifically, **this bill would**:

1) Require the Office of Emergency Services (Cal OES) to establish and lead the Cal-CSIC, and require the Cal-CSIC to develop a cybersecurity strategy for California informed by recommendations by the Cybersecurity Task Force, as specified, and requires Cal-CSIC to operate in close coordination with the California State Threat Assessment System and the U.S. Department of Homeland Security—National Cybersecurity and Communications Integration Center, as specified.

2) Specify that the primary mission of the Cal-CSIC is 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.

3) Specify that the membership of the Cal-CSIC shall include representatives of Cal OES, the Office of Information Security (OIS); the State Threat Assessment Center; the Department of the California Highway Patrol (CHP); the California Military Department (CMD); the Office of the Attorney General; the California Health and Human Services Agency; the California Utilities Emergency Association; the California State University; the University of California; the California Community Colleges; the U.S. Department of Homeland Security; the U.S. Federal Bureau of Investigation; the U.S. Secret Service; the U.S. Coast Guard; and other members as designated by the Director of Cal OES.

4) Specify that the cybersecurity strategy developed by Cal-CSIC shall be developed to improve how cyber threats are identified, understood, and shared in order to reduce threats to California government, businesses and consumers. The strategy would also be required to strengthen cyber emergency preparedness and response, standardize implementation of data protection measures, enhance digital forensics and cyber investigative capabilities, deepen expertise among California's workforce of cybersecurity professionals, and expand cybersecurity awareness and public education.

5) Requires Cal-CSIC to establish a Cyber Incident Response Team, as specified, 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, as well as assist law enforcement agencies with primary jurisdiction for cyber-related criminal investigations and agencies responsible for advancing information security within state government.

EXISTING LAW:

1) Authorizes the Governor to make, amend, and rescind orders and regulations to implement the California Emergency Services Act. (Gov. Code Sec. 8550 *et seq.*) The Act requires the Governor to coordinate the State Emergency Plan and those programs necessary for the mitigation of the effects of an emergency in this state. (Gov. Code Sec. 8569.) The Act creates within the office of the Governor the Cal OES, which is responsible for the state's emergency and disaster response services, as specified. (Gov. Code Sec. 8585.)

2) Requires, by Executive order in 2015, Cal OES to establish and lead the Cal-CSIC, with its 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 the state. (Executive Order B-34-15.)

3) Requires, by Executive order, that the Cal-CSIC be comprised of representatives from various entities, and that it develop a statewide cybersecurity strategy informed by recommendations from the California Task Force on Cybersecurity and in accordance with state and federal requirements, standards, and best practices. (Executive Order B-34-15.)

4) Establishes the California Department of Technology (CDT) within the Government Operations Agency, under the supervision of the Director of Technology, also known as the State Chief Information Officer. (Gov. Code Sec. 11545(a).) Establishes within CDT the OIS, the duties of which shall be to provide direction for information security and privacy to state government agencies, departments, and offices, as specified. (Gov. Code Sec. 11549.)

5) Requires state entities to implement the information security and privacy policies, standards and procedures issued by the OIS. (Gov. Code Sec. 11549.3(b).) Authorizes OIS to conduct, or require to be conducted, an independent security assessment (ISA) of every state agency, department, or office, as specified. State agencies and entities required to conduct or receive an ISA pursuant to those provisions are required to transmit the complete results of that assessment and recommendations for mitigating system vulnerabilities, if any, to OIS and Cal OES. (Gov. Code Sec. 11549.3(c), (d).) Further requires OIS to report to CDT and Cal OES any state entity found to be noncompliant with information security program requirements, and also requires OIS to notify Cal OES, CHP, and the Department of Justice regarding any criminal or alleged criminal cyber activity affecting any state entity or critical infrastructure of state government. (Gov. Code Sec. 11549.3(e), (h).)

6) Authorizes the CMD to perform an ISA of any state agency, department, or office, the cost of which shall be funded by the state agency, department, or office being assessed. (Gov. Code Sec. 11549.3(c)(3).)

7) Requires OIS to consult with the Director of Technology, the Cal OES, the Director of General Services, the Director of Finance, and any other relevant agencies concerning policies, standards, and procedures related to information security and privacy. (Gov. Code Sec. 11549.4.)

FISCAL EFFECT: Unknown

COMMENTS:

Purpose of the bill: According to the author: "This bill is needed because the importance and need for the Cal-CSIC, and in general a coordinated state response structure for cybersecurity, is only increasing. Over the course of the past six months since the Governor's veto [of AB 1306 (Obernolte), 2016)], the Cal-CSIC has made significant strides in developing its capabilities and mission. With the Cal-CSIC's continued existence directly connected to the pleasure of the sitting Governor, and Gov. Brown's tenure soon coming to a close, [this bill represents an attempt to] re-engage in a discussion with the Executive Branch about the benefits of placing core provisions providing for the Cal-CSIC into statute before a new administration comes into office.

Additionally Cal OES has published both the 'Cyber Incident Response Guide for the State of California' and 'California Joint Cyber Incident Communications and Escalation Framework' that are intended in part to constitute the Emergency Support Function 18 'Cybersecurity' of the State Emergency Plan. These documents place the Cal-CSIC in important roles in planning for, and responding to cyber incidents. All other partners under the Response Guide and Communication Framework have statutory mandates to participate to some degree in state information security and are all allocated budget funds (CDT, CMD, CHP), leaving Cal-CSIC as the component with the most near and long-term uncertainty in addressing the state's long term cybersecurity goals.

Testimony from the recent Joint Oversight Hearing, from CDT's annual report, and other briefings provided by the Executive Branch to Legislature makes clear that cyber threats to the state government network, both private and public critical infrastructure, and other Cal-CSIC partners is on the rise. These threats are becoming more sophisticated and require large amounts of information-sharing to detect trends and allocated response resources. This is a core service of the Cal-CSIC and [it] would be difficult if not impossible in the short-term for any one of the other core four partners to take on the service offerings of the Cal-CSIC if it were to be discontinued by a future Governor."

Background: In 2009, the California Legislature merged the powers, purposes, and responsibilities of the former Cal OES with those of the Office of Homeland Security (OHS) into the newly- created California Emergency Management Agency (CalEMA).On July 1, 2013, Governor Edmund G. Brown Jr.'s Reorganization Plan #2 eliminated CalEMA and restored it to the Governor's Office, renaming it the California Governor's Office of Emergency Services (Cal OES), and merging it with the Office of Public Safety Communications. Today, Cal OES is responsible for overseeing and coordinating emergency preparedness, response, recovery and homeland security activities within the state.

Additionally, CESA authorizes the Governor to take actions to prepare for, respond to, and prevent natural or human-caused emergencies that endanger life, property, and the state's resources, and further authorizes Cal OES and its Director to take actions to coordinate emergency planning, preparedness, and response activities. On August 31, 2015, Governor Brown, under the authority of CESA, signed Executive Order B-34-15.

Executive Order B-34-15 (EO): Governor Brown signed Executive Order B-34-15 (EO) which noted the increasing number and complexity of cyberattacks against public and private networks, and in response announced the establishment of the California Cybersecurity Integration Center (Cal-CISC).

Cal-CISC is charged with reducing the likelihood and severity of a damaging cyber incident in

California, and would serve as the "central organizing hub" of state government's cybersecurity activities and coordinate information sharing" with a variety of government agencies. It would be comprised of representatives from 15 different state and federal public entities.

Its main purposes would be threat information sharing, risk assessment, threat prioritization, supporting governmental audits and accountability measures, enabling cross-sector coordination and sharing of best practices. Cal-CISC would be responsible for developing a statewide cybersecurity strategy. It would also be charged with establishing a Cyber Incident Response Team (CIRT) 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. CIRT would also provide assistance to law enforcement agencies with primary jurisdiction over cyber-crimes and state government cybersecurity. The team would be populated with staff from the agencies, departments and organizations represented on Cal-CISC.

Cal-CSIC: In April 2016, CalOES placed the Cal-CSIC alongside the State Threat Assessment Center (STAC), California's information sharing clearinghouse of strategic threat analysis and situational awareness reporting. This co-location ensured immediate collaboration across the State Threat Assessment System, California's intelligence community.

According to Cal OES, since April of 2016, "Cal-CSIC representatives from Cal OES, the California Department of Technology, the California Military Department, and the California Highway Patrol [have been] pooling resources to implement cyber vulnerability assessments and develop intuitive cyber threat alerts for the end-user. California receives a great deal of cyber threat information from other local, state, and national partners, but rarely receive a strategic look at the motivations behind these threats and the techniques to prevent, mitigate, or respond to them. The Cal-CSIC endeavors to provide useful information that will help protect California's residents and infrastructure."

"Furthermore, Cal-CSIC personnel are working to identify best and cost-effective technological solutions to augment the state's cybersecurity mission and protect the privacy and civil liberties of California's residents. The Cal-CSIC seeks to instill trust and confidence by promoting transparency of internal processes and protocols, and maintaining confidentiality and integrity while exchanging cybersecurity information with its partners."

Try again: This bill is very similar to a prior bill, AB 1306 (Obernolte, 2017), which also sought to codify the Cal-CSIC. AB 1306 was ultimately vetoed by Governor Brown with the following message:

"Two years ago I established the California Cybersecurity Integration Center when I signed Executive Order B-34-15. Cybersecurity threats against the state are constantly changing and the Center continues to mature in response to these threats. I am concerned that placing the Center in statute as this bill proposes to do, will unduly limit the Center's flexibility as it pursues its mission to protect the state against cyberattacks."

AB 1306, however, did not include substantial portions of the Executive Order that are contained in this bill, including the right of the Cal OES Director to designate additional members; provisions directing Cal-CSIC to assist in threat information sharing, provide attack warnings to stakeholders, assess risks to critical infrastructure, prioritize cyber threats, and support security assessments and audits; provisions related to the establishment of a CIRT unit; and the

requirement that information sharing be conducted in a manner that protects the privacy and civil liberties of individuals, safeguards sensitive information, and preserve business confidentiality.

Another key difference between this bill and AB 1306 is that this bill does not contain any of the AB 1306 provisions that would have provided specific direction to Cal OES regarding the expenditure of federal grant money for cybersecurity purposes. That AB 1306 language essentially sought to formally authorize the Cal OES Director to administer, authorize and allocate federal homeland security grant funding, and to require the Director to prioritize the use of that grant funding (except in state emergencies) for preventive measures taken by OIS to ensure compliance by state departments and agencies with existing information security standards and policies, including the performance of risk assessments. That being said, there was no obvious reason to believe that the Director of Cal OES lacks the authority to administer and allocate such federal grants, as the Director has presumably been administering such grants for years.

Double Referral: AB 2813 will be first heard in Assembly Committee on Privacy and Consumer Protection on April 17, 2018.

Related legislation: AB 1306 (Obernolte) of 2017/2018 Session. Would have established the Cal-CSIC, require it to develop a cybersecurity strategy for California, and authorize the administration of federal homeland security grant funding by OES. (Vetoed by Governor)

AB 2595 (Linder) of 2015/2016 Session. Would have established the Cal-CSIC, require it to develop a cybersecurity strategy for California, and authorize the administration of federal homeland security grant funding by OES. (Held in the Assembly Appropriations Committee.).

AB 1841 (Irwin) Chapter 508, Statutes of 2016. Requires CalOES to develop, by July 1, 2017, a statewide emergency services response plan for cybersecurity attacks against critical infrastructure, and further requires OES to develop a comprehensive cybersecurity strategy by July 1, 2018, with which all state agencies must report compliance by January 1, 2019.

AB 1881 (Chang) of 2015/2016 Session. Would have required the Director of the California Department of Technology to develop and update mandatory baseline security controls for state networks based on industry and national standards, and annually measure the state's progress towards compliance. (Held in the Assembly Appropriations Committee.).

SB 949 (Jackson) of 2015/2016 Session. Would have authorized the Governor to require owners and operators of critical infrastructure to submit critical infrastructure information to OES or any other designee for the purposes of gathering, analyzing, communicating, or disclosing critical infrastructure information. (Died in Senate Governmental Organizations Committee)

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

Analysis Prepared by: Kenton Stanhope / G.O. / (916) 319-2531