Date of Hearing: April 19, 2017

ASSEMBLY COMMITTEE ON GOVERNMENTAL ORGANIZATION
Adam Gray, Chair
AB 1306 (Obernolte) – As Amended April 6, 2017

SUBJECT: California Cybersecurity Integration Center

SUMMARY: Establishes the California Cybersecurity Integration Center (Cal-CSIC), requires it to develop a cybersecurity strategy for California, and the Director of Emergency Services (Director) to administer federal grant money for cybersecurity prevention measures. Specifically, **this bill**:

1) Establishes the Cal-CSIC within the Governor's Office of Emergency Services (CalOES), and requires the Cal-CSIC to develop a cybersecurity strategy for California in coordination with the Cybersecurity Task Force, as specified.

2) Specifies 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) Specifies that the membership of the Cal-CSIC shall include representatives of CalOES, the Department of Technology's Office of Information Security (OIS); the State Threat Assessment Center; the Department of the California Highway Patrol; the California Military Department; 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; and the California Community Colleges.

4) Authorizes the Director, in consultation with OIS or the Cybersecurity Task Force, or both, to administer, authorize, and allocate federal homeland security grant funding in accordance with federal grant guidelines and shall prioritize grant funding for prevention measures undertaken by OIS in furtherance of the provision in the Governor's Executive Order B-34-15 that directs state departments and agencies to "ensure compliance with existing information security and privacy policies, promote awareness of information security standards with their workforce."

5) Clarifies that the provisions of this bill do not preclude the Director from administering the grant programs to respond to statewide emergencies requiring immediate attention.

6) Defines the terms "prevention measures" and "federal homeland security grant funding."

EXISTING LAW:

1) Establishes CalOES by the Governor's Reorganization Plan No.2, operative July 1, 2013.

2) Requires CalOES to perform a variety of duties with respect to specified emergency preparedness, mitigation, and response activities in the state, including emergency medical services.

3) Requires the Governor and CalOES, pursuant to the California Emergency Services Act (CESA), to prepare for and mitigate the effects of emergencies in the state.

4) Requires CalOES, and its appointed Director, to perform a variety of duties with respect to specified emergency preparedness, mitigation, and response activities in the state, including emergency medical services.

5) Requires, by Executive order in 2015, CalOES 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)

6) 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)

7) Establishes, within the California Department of Technology (CDT), the Office of Information Security to ensure the confidentiality, integrity, and availability of state systems and applications, and to promote and protect privacy as part of the development and operations of state systems and applications to ensure the trust of the residents of this state.

FISCAL EFFECT: Unknown

COMMENTS:

Purpose of the Bill: According to the author, "Cybersecurity is a growing concern to our state. We must do everything we can as a state to be prepared for a possible attack. Cal-CSIC has been a vital part of the state's response plan and it is time to codify the organization to make sure they will be around to assess threats and prepare for attacks. Additionally, we should be prioritizing our cybersecurity grant dollars for the prevention measure that are in line with our cybersecurity readiness goals. Finally, in the unfortunate case of a response to a cyber-attack becoming necessary, the California Department of Technology should absolutely be outlined in the Emergency Plan."

Background: In 2009, the California Legislature merged the powers, purposes, and responsibilities of the former CalOES 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 (CalOES), and merging it with the Office of Public Safety Communications. Today, CalOES 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 CalOES 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 CalOES, 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."

Homeland Security Grant Funding**:** According to the author, the most recent publicly available figures show that a total of $193 million in homeland security grants have been allocated for California. The State Homeland Security Program ($60.2 million) assists state, tribal and local preparedness activities that address high-priority preparedness gaps across all core capabilities and mission areas where a nexus to terrorism exists. The Urban Areas Security Initiative ($124.7 million) assists high-threat, high-density urban areas in efforts to build and sustain the capabilities necessary to prevent, protect against, mitigate, respond to, and recover from acts of terrorism. Operation Stonegarden ($9.4 million) supports enhanced cooperation and coordination among Customs and Border Protection, United States Border Patrol, and local, Tribal, territorial,

state, and federal law enforcement agencies and funds investments in joint efforts to secure the United States borders along routes of ingress from international borders to include travel corridors in states bordering Mexico and Canada, as well as states and territories with international water borders.

As noted by the Committee on Privacy and Consumer Protection, the practical effect of the language of this bill is to authorize the Director of CalOES to administer, authorize and allocate federal homeland security grant funding, and to prioritize that grant funding (except in state emergencies) for preventative 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. There is no clear reason to believe that the Director of CalOES lacks the authority to administer and allocate such federal grants, as such administration has been ongoing for years.

Policy Considerations:

1. Should AB 1306 become law, it would place only a portion of the EO in statute. As stated above, the Governor, under the authority of CESA, signed B-34-15, thus, the contents in the EO do not need to be codified in statute for the directions/orders of the Governor to be realized. However, it certainly does not hurt and could provide for additional accountability for all involved agencies and remove the Governor's authority to unilaterally change any of the provisions added to statute. *The Committee may wish to consider whether it is necessary to codify the EO in statute. If yes, the Committee and author may wish to consider adding the entire EO into statute.*

2. Should AB 1306 become law, it would bill authorize the Director of CalOES to administer, authorize and allocate federal homeland security grant funding. As stated above, there is no clear reason to believe that the Director lacks the authority to administer and allocate said federal grant funds. *Should the intent of AB 1306 be to provide more transparency or allocation control of federal homeland security grants funds, the Committee and author may wish to consider whether or not more specific provisions related to transparency or allocation control is appropriate, such as a requirement to annually report online any expenditures or allocations of federal homeland security grants funds.*

Double Referral: AB 1306 was first heard in Assembly Committee on Privacy and Consumer Protection on March 28, 2017, and passed on a 9-1 vote.

Related legislation: 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