Date of Hearing: April 25, 2023

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
AB 1667 (Irwin) – As Amended March 16, 2023

Proposed Consent

SUBJECT: Department of Technology: California Cybersecurity Awareness and Education Council

SYNOPSIS

Among the cybersecurity challenges that California faces are, first, ensuring that the state's residents are more aware of what they could be doing individually and in their households, to make themselves less vulnerable to cyber threats; and second, developing a much-needed cybersecurity workforce for the state.

In response, this bill, sponsored by Common Sense Media, would establish the California Cybersecurity Awareness and Education Council, consisting of 15 members representing a wide range of backgrounds, including K-12 education (both teachers and students), business, academia, public safety, and the nonprofit sector.

The Council would be responsible for researching how to increase cybersecurity awareness generally, and how to educate students, families, and adults in improved cybersecurity practices. The Council would also be tasked with researching ways to create a larger and more diverse cybersecurity-trained workforce.

This research, in turn, would lead to a Council proposal for a strategy to engage Californians in the effort to improve cybersecurity practices and strengthen cyber infrastructure, including through a public awareness campaign and education materials.

This bill appears well-designed to deliver policy proposals to the Legislature and the Administration as to how to attack the problems of cybersecurity awareness and education, as well as training a skilled cybersecurity workforce. The Council's work could be an important source of future policy ideas for improving the state's overall cybersecurity on a number of levels.

SUMMARY: Establishes the California Cybersecurity Awareness and Education Council, tasked with proposing a strategy to engage Californians in an effort to improve cybersecurity practices, strengthen cyber infrastructure, and create a larger and more diverse cybersecurity-trained workforce. Specifically, **this bill**:

1) Establishes the California Cybersecurity Awareness and Education Council (Council) within the California Department of Technology (CDT).

2) Declares that the Council shall be composed of 15 members, five of whom shall be selected by the Speaker of the Assembly, five of whom shall be selected by the President pro Tempore of the Senate, and five of whom shall be appointed by the Governor.

3) Encourages the selection of Council members who represent a wide range of stakeholders, including, but not limited to:

    a) Teachers or other K–12 public school representatives.

    b) High school students or other youth leaders.

    c) Business owners.

    d) Academic cybersecurity experts.

    e) Public safety leaders.

    f) Nonprofit organization representatives.

4) Tasks the Council with researching both of the following:

    a) Ways to increase cybersecurity awareness and education of students, families, and other adults, with the goal of helping people learn and use healthy cybersecurity practices.

    b) Ways to create a larger and more diverse cybersecurity-trained workforce.

5) Requires the Council to propose a strategy to engage Californians in the effort to improve cybersecurity practices and strengthen cyber infrastructure. The strategy is to focus on, but not be limited to, both of the following:

    a) Basic cybersecurity education for individuals, families, schools, and workplaces.

    b) A public awareness campaign and education materials aimed at ensuring that more Californians become aware of cybersecurity's importance.

6) Requires the Council to deliver a report to the Speaker of the Assembly, the President pro Tempore of the Senate, the Governor, the Director of Technology, the Superintendent of Public Instruction, and the Director of Emergency Services that includes, but is not limited to, all of the following:

    a) Approaches that the state can take to raise awareness and increase education of cybersecurity, including in K–12 schools, institutions of higher education, and workplaces.

    b) Ways to effectively utilize social media, marketing campaigns, and the news media to increase awareness of and distribute materials about cybersecurity.

    c) Ways to balance amplifying existing resources and work that is already being done to promote cybersecurity awareness with creating new resources and partnerships.

    d) Ways to reach out to underrepresented populations, including, but not limited to, low-income communities and individuals who speak languages other than English.

    e) Ways in which Californians can communicate with appropriate government officials about cybersecurity concerns.

f) Other recommendations that the Council deems appropriate.

7) Repeals this measure as of January 1, 2026.

EXISTING LAW:

1) Establishes the California Department of Technology in the Government Operations Agency. (Gov. Code § 11545.)

2) Directs the California Cybersecurity Integration Center to develop a statewide cybersecurity strategy, which, among other goals, is meant to deepen expertise among California's workforce of cybersecurity professionals, and expand cybersecurity awareness and public education. (Gov. Code § 8586.5(c))

3) Establishes the Cybersecurity Regional Alliances and Multistakeholder Partnerships Pilot Program through the California State University System. (Educ. Code § 89270.)

FISCAL EFFECT: As currently in print this bill is keyed fiscal.

COMMENTS:

1) **Background.** The Cybersecurity and Infrastructure Security Agency (CISA), the federal agency tasked with leading the nation's cybersecurity efforts, has defined the term "cybersecurity" to mean "the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information." (CISA, *What is Cybersecurity?* (Feb 1, 2021), *available at* https://www.cisa.gov/news-events/news/what-cybersecurity.) Given that computer networks touch nearly every aspect of modern life, potential vulnerabilities to cyberattack are present at the level of national, state, and local government; in businesses, nonprofits, and other private-sector entities; and in our homes and on our smartphones. With the advent of the "Internet of Things," hackers even threaten to compromise everyday home appliances and vehicles.

Given the universality of cyber threats, no single entity can be relied upon to ensure cybersecurity; instead, protective measures are needed at every level. Lest this sound extreme, consider an analogy to the ongoing need to ensure fire safety. Individuals have to be careful not to burn themselves or start fires while cooking; apartments and houses are required to install smoke alarms; commercial buildings are well-stocked with fire extinguishers; there are fire hydrants on many streets, and fire stations within driving distance of most buildings in cities and counties; the state fights wildfires; and the federal government safeguards against terrorist attacks. One cannot reasonably claim that it is the sole responsibility of government or of particular businesses to protect against fire. Similarly, as time goes on, it is clear that reasonable, cost-effective actions can (and increasingly, must) be taken at every level to help ensure cybersecurity.

This bill would further the goal of enhancing statewide cybersecurity at all levels by establishing the California Cybersecurity Awareness and Education Council within the California Department of Technology. The Council is meant to improve efforts at the state level, first, to ensure individual and household awareness of the need for cybersecurity; second, to communicate cybersecurity best practices to individuals and households; and third, to help train a much-needed cybersecurity workforce.

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

> Cybersecurity awareness and training is something every Californian needs to be able to navigate our ever increasing connected lives. While efforts have been made to increase the pipeline and provide guidance to Californians, we still see cyberattacks on the rise. While the secure design and configuration of our devices and networks is important, the user will continue to be the weakest link until we achieve widespread cybersecurity awareness.

3) **The need for this bill.** Younger Californians face numerous cybersecurity threats, including data theft, mobile device malware, and "camfecting," where hackers are able to remotely access and take control of their webcams. (UC Berkeley Extension Cybersecurity Boot Camp, *Cybersecurity in Education: What Teachers, Parents and Students Should Know, available at* https://bootcamp.berkeley.edu/blog/cybersecurity-in-education-what-teachers-parents-and-students-should-know/#cybersecurity-for-students.)

Cybersecurity threats also loom in the home. Users may forget to apply updates to their PC's operating system or their home routers, leading to their networks being hacked. Conversations, including those involving sensitive work-related topics, may be overheard by voice-activated home assistants and transmitted to external servers. Passwords may simply be too weak and easily guessed. (National Security Agency, *Cybersecurity Information Sheet, available at* https://media.defense.gov/2023/Feb/22/2003165170/-1/-1/0/CSI_BEST_PRACTICES_FOR_SECURING_YOUR_HOME_NETWORK.PDF.)

Cyberseek, a collaborative public-private project to help close the cybersecurity skills gap, estimates that there are currently 561,743 job openings requiring cybersecurity-related skills. Data shows that 81,584 of these are in California. (Cyberseek, *Cybersecurity Supply/Demand Heat Map, available at*https://www.cyberseek.org/heatmap.html.)

4) **What this bill would do.** The California Cybersecurity Awareness and Education Council (Council) established by this bill would consist of 15 members, representing a wide range of backgrounds, including K-12 education (both teachers and students), business, academia, public safety, and the nonprofit sector.

This bill would ensure that the Council plays an active role in addressing both of the challenges outlined above. First, the Council would be tasked with researching how to increase cybersecurity awareness generally, as well as how to educate students, families, and adults in healthy cybersecurity practices. The Council would also be tasked with researching ways to create a larger and more diverse cybersecurity-trained workforce.

This research, in turn, would lead to a Council proposal for a strategy to engage Californians in the effort to improve cybersecurity practices and strengthen cyber infrastructure, including through a public awareness campaign and education materials.

The Council would be required to report its strategy to the Legislature, the Governor, the Director of Technology, the Superintendent of Public Instruction, and the Director of Emergency of Services. The report would have to include the information set forth in paragraph 6) of the **SUMMARY** above.

This bill appears well-designed to deliver policy proposals to the Legislature and the Administration as to how to attack the problems of cybersecurity awareness and education, and

how to train a skilled cybersecurity workforce. As such, it could be an important source of future policy ideas for improving the state's overall cybersecurity on a number of levels.

5) **Related legislation.** AB 749 (Irwin, 2023) would require every state agency to implement Zero Trust architecture by January 1, 2025, including multifactor authentication, enterprise endpoint detection and response solutions, and robust logging practices, following uniform technology policies, standards, and procedures developed by the Chief of the Office of Information Security. Status: Assembly Appropriations.

AB 2135 (Irwin, Chap. 773, Stats. 2022) required state agencies not 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. It also requires those agencies to perform a comprehensive independent security assessment every two years, as specified.

AB 183 (Budget, Chap. 54, Stats. 2021) established the Cybersecurity Regional Alliances and Multistakeholder Partnerships Pilot Program, intended to address the cybersecurity workforce gap.

AB 2564 (Chau, 2020) would have stated the Legislature's intent to enact legislation to improve the security of information technology systems and connected devices by requiring public agencies and businesses to develop security vulnerability disclosure policies. The bill died without being referred to Committee.

ARGUMENTS IN SUPPORT: Bill sponsor Common Sense Media explains the need for this bill:

> Cybersecurity is widely recognized as an under-addressed threat to our economy, national security, and personal safety. […] While governments and large institutions bear the greatest responsibility for hardening America's cyber infrastructure, there is also an important role to play for everyday Americans. Families and individuals can keep their online information and networks safe by taking basic but important steps such as using strict privacy settings on apps and websites, enabling multi-factor authentication, using a password manager, learning about and staying cautious of phishing scams, regularly updating software, and more. And, the more that individuals practice clean cyber hygiene, the more secure our country's overall cyber infrastructure will be. AB 1667 addresses the need for engaging all Californians to increase education of healthy cybersecurity hygiene.

REGISTERED SUPPORT / OPPOSITION:

Support

Common Sense Media (sponsor)

Opposition

None on file

Analysis Prepared by: Jith Meganathan / P. & C.P. / (916) 319-2200