Date of Hearing: April 23, 2019

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 1566 (Chau) – As Amended March 28, 2019

SUBJECT: California Cyber Range Pilot Project

SUMMARY: This bill would establish the California Cyber Range Pilot Project, administered by the California Cybersecurity Institute (CCI), to establish a cloud-hosted exercise area environment for hands-on cybersecurity labs and exercises for pupils and students, through a year-long multiphased effort, as specified. The bill would require the pilot project to produce a scalable model for a permanent California Cyber Range Program. Specifically, **this bill would**:

1) Establish the California Cyber Range Pilot Project under the administration of the California Cybersecurity Institute, to test the overall feasibility of the pilot project through a yearlong, multiphased effort. The pilot project shall be hosted by one to three campuses of the California State University (CSU) or University of California (UC).

2) Require that the selected CSU or UC campus(es) do all of the following:

    - Establish a cloud-hosted exercise area environment for hands-on cybersecurity labs and exercises for pupils and students. This bill would authorize this effort to adapt cyber range cloud technology adopted in other states, such as the Commonwealth of Virginia, to serve typical state educational scenarios in a statewide format.

    - Test and validate the curriculum to ensure it meets the state's computer science strategic implementation plan, developed pursuant to specified existing law, to establish an extensive courseware repository for educators in the cyber range program.

    - Validate the economic viability of the cyber range program and capture long-term acquisition and administrative expenses associated with operations.

3) Require that the pilot project produce a scalable model for a permanent California Cyber Range Program with representative curriculum and analysis for establishing curricular enhancements and required operating expenses necessary for a statewide rollout of the cyber range.

4) Specify that eligible applicants for the pilot project would be a small number of: (a) schools operating programs from kindergarten through grades 1 to 12, inclusive; (b) community colleges; and, (c) public universities. It would further specify that additional schools may be added to the pilot project based on recommendations by the CCI project administrators.

5) Include various findings and declarations, including the following:

    - With over 300,000 cybersecurity openings across the country and over 35,000 open positions in the state, a pipeline of future defenders needs to be developed.

- The state should engage all students in topics such as computer science, coding, and more, as part of its basic curriculum and to actively promote career development in areas such as information technology and cybersecurity.

- At the same time, more and more states are turning to new technology and nontraditional pathways to develop and deliver a cybersecurity workforce.

- It is appropriate to enact legislation that establishes a pilot project to examine and ensure the state is properly positioned to train the current and next generations' cyber workforce and to leverage existing technology to reach that goal in an expeditious and cost-effective manner.

EXISTING LAW:

1) Requires, until July 31, 2020, that the Superintendent of Public Instruction convene a computer science strategic implementation advisory panel with a specified membership to develop and submit recommendations for a computer science strategic implementation plan to the Superintendent, the State Board of Education, and the Legislature, as specified. (Ed. Code Sec. 53310 et seq.)

2) Requires the CSU, and requests the UC, to establish a model uniform set of academic standards for computer science high school courses for the purposes of recognition for admission, and to develop and implement a speedy process whereby high schools may obtain approval of their courses to satisfy specified admissions requirements. (Ed. Code Sec. 66205.5.)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of this bill**: This bill seeks to establish a pilot project that will study, test, and establish a cybersecurity education program (a "Cyber Range") in California that can help teach, train, and test the state's students and public employees, and ultimately, develop California's future workforce by way of a virtual and secure "sandbox." This is an author-sponsored bill.

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

> California is the 5th largest economy in the world, yet Cybersecurity training and education is a pressing issue in the state. According to Cyberseek.org, California and the entire nation have a serious cybersecurity workforce challenge. There are over 300,000 cybersecurity openings across the country and over 35,000 positions in California. More and more states are turning to new technology and non-traditional pathways to develop and deliver a cybersecurity workforce.
>
> The issue of developing a future pipeline of workers is not unique to California. Virginia and a consortium of its leading universities have developed an innovative cyber range solution to support cybersecurity education across the state and across public high schools, colleges, and universities.

For example, the Virginia Cyber Range seeks to increase the number of fully prepared students entering the cybersecurity workforce in operations, development, and research. The Cyber Range provides an extensive Courseware Repository for educators and a cloud-hosted exercise area environment for hands-on cybersecurity labs and exercises for students.

The Virginia Cyber Range was developed with an initial grant from the Virginia Governor of $2M and is now supported by a portfolio of over $60M in funding.

The Virginia Cyber Range could be replicated to cover California at a small fraction of Virginia's cost and could accelerate cybersecurity training and education across our schools from K-12, colleges and universities. It would also be a powerful tool in cybersecurity training of California's state employees. […]

AB 1566 will establish a pilot project, administered by the California Cybersecurity Institute, to examine and ensure the state is properly positioned to train the current and next generations' cyber workforce by testing, studying, and evaluating the feasibility and adaptability of the Cyber Range to California.

3) **Department of Defense "cyberspace sandbox**": This bill's proposal to establish a cyber range in California is an idea that draws largely from the Virginia Cyber Range (discussed in Comments 2 and 4), but shares roots with other cyber training sandboxes created for employees to test and evaluate new cyber technologies and defense tactics. On the federal level, for example, the Department of Defense (DoD) established a "cyberspace sandbox" for training exercises and for testing the limits of software applications roughly a decade ago. That Defense Department Information Assurance Range was "designed to provide an operationally realistic simulation of the Global Information Grid, its network services and information assurance/network defense capabilities in a closed environment. It also serves as a virtual training ground for DOD cyber personnel and a testing and evaluation space for new information assurance and network defense technologies, tactics and policies." (Kenyon, *New DOD test range serves as cyber training ground*, Defense Systems (Dec. 2, 2010) <https://defensesystems.com/articles/2010/12/01/dod-launches-cyber-test-range.aspx> [as of Apr. 3, 2019].)

4) **Virginia Cyber Range Background**: First proposed by Virginia's then-Governor Terry McAuliffe in late 2015, the Virginia Cyber Range sought to take what was described as "an important step to develop the workforce needed to keep data and systems safe from cyber threats" as online attacks on financial, research, and consumer data become more sophisticated and urgent. Together with eight other public institutions of higher education across that state, Virginia Tech led the effort to create the state-of-the-art platform for cybersecurity education to provide advanced cybersecurity training exercises for high-school and college students. (Virginia Tech Daily, *Virginia Cyber Range to enhance cybersecurity education across the Commonwealth* (Sept. 21, 2016).)

The project's initial focus will be on serving community colleges and four-year institutions with offerings that will include modules for use in college courses, laboratory exercises and projects, and realistic tactical cybersecurity trials that can supplement existing courses. Students will gain knowledge of digital forensics, network defense, how to secure critical infrastructure and the "internet of things," malware detection, usability

> and privacy issues, and secure coding practices. The project is expected to evolve to also serve K-12 students and other groups within the commonwealth.
>
> The Cyber Range will largely operate as a virtual center. Offerings will be crafted and hosted in the "cloud," where they can be accessed by participating schools and agencies. This approach will allow for easy customization, scalability, and responsiveness, while minimizing costs. (*Id*.)

Stated another way, the Virginia Cyber Range is a hands-on laboratory that provides students access to hands-on lab exercises through their web browsers. As described by a March 2017 Virginia Business article, the cyber range grew into a training platform for the entire state based on a partnership with Amazon Web Services (AWS):

> The partnership with AWS will help the cyber range expand for use by students at universities and colleges across Virginia, as well as to high school students by fall 2017.
>
> "The benefit of that is that the school doesn't have to host [the technology] themselves," says David Raymond, director of the Virginia Cyber Range. "Normally to do this sort of thing you would purchase a bunch of servers, you'd install a bunch of software, you'd have system administrators that you pay to keep this environment up and running. With the Virginia Cyber Range, we can provide this resource across the commonwealth."
>
> That will especially be helpful to cybersecurity classes being offered to high school students, where the expense required to create these types of hands-on training is prohibitive. The range is planning to expand to high school students through teacher trainings and cybersecurity camps offered this summer.
>
> Courses and labs are created by faculty and are available to other educators using the site, says Raymond. It also gives students easy web access to training, whereas they previously might need high-powered laptops or computers in a lab.
>
> The Virginia Cyber Range is supported with $2 million in Virginia's current two-year budget and is designed to grow Virginia's cybersecurity workforce. (Virginia Business, *Virginia Cyber Range to grow under new agreement* (Mar. 1, 2017) <http://www.virginiabusiness.com/reports/article/virginia-cyber-range-to-grow-under-new-agreement> [as of Apr. 3, 2019].)

Today, the Virginia Cyber Range is "entirely state-funded and based out of Virginia Tech's Corporate Research Center, but largely operates as a virtual center that K-12 and higher ed[ucation] classrooms in Virginia can log onto and access an ever-growing curriculum of cybersecurity lessons. Agencies and industry organizations can also schedule training and use the environments that the cyber range provides." (Johnston, *Cyber ranges are all the rage at these universities*, EdScoop (Feb. 26, 2018) <https://edscoop.com/cyber-ranges-universities-virginia-florida-georgia-arkansas-michigan/> [as of Apr. 3, 2019]; hereinafter "Johnston".)

Largely inspired by that program, this bill would establish the California Cyber Range Pilot Project under the administration of the California Cybersecurity Institute, to test the overall feasibility of the pilot project through a yearlong, multiphased effort. One to three CSU or UC campuses would host the pilot project, with the responsibility to do all of the following:

- establish a cloud-hosted exercise area environment for hands-on cybersecurity labs and exercises for pupils and students;

- test and validate the curriculum to ensure it meets the state's computer science strategic implementation plan, developed pursuant to specified existing law, to establish an extensive courseware repository for educators in the cyber range program; and,

- validate the economic viability of the cyber range program and capture long-term acquisition and administrative expenses associated with operations.

As stated by the author, "[t]he Cyber Range represents a critical step in ensuring California is positioned to train the next generation of cyber workforce by leveraging existing technology for an expeditious and cost-effective solution."

5) **Other states are following in Virginia's footsteps to provide cybersecurity education and training, and to close the gap in their workforce needs, by way of cyber ranges**: While Virginia's cyber range program is relatively young, in the last several years, many other states have established or stated the process of establishing their own cyber ranges. For example, in 2017, the Western Washington University (WWU) campus at Poulsbo set out to host Washington state's first cyber range. Describing it as a shooting range for cyber security personnel, one article explained the range's capacity to provide training, as follows:

> "Cyber ranges function like shooting or kinetic ranges, facilitating training in weapons, operations or tactics. Thus, cyber warriors and IT professionals employed by various agencies train, develop and test cyber range technologies to ensure consistent operations and readiness for real world deployment," according to Techopedia […].
>
> Cyber ranges – (closed clouds" that are cut off from the real web – "allow students to be black hats and do things that, if they did them on the real web, would be illegal and they would wind up in jail," [Erik] Fretheim [WWU's program director for computer information systems security, who is responsible developing the range] said. […] By isolating a realistic representation of the Internet, it is possible to test advanced tactics, techniques, and procedures – playing the role of friendly or adversary forces, or neutral networks (e.g. a utility company) – in a variation of highly realistic conditions and situations.
>
> Merit […] which operates the University of Michigan cyber range likens it to a "secure sandbox … a flexible, secure environment that can be used for cybersecurity education, training exercises, and software testing. Located in a virtual cloud, the Secure Sandbox simulates a real-world networked environment with virtual machines that act as web servers, mail servers, and other types of machines. Utilizing the virtual town of Alphaville, the Michigan Cyber Range conducts hands-on cybersecurity exercises to help teams practice and prepare for any type of data breach." (Asla, *Poulsbo cyber range is a first for Washington*, Kitsap Daily News (Mar. 26, 2017).)

In the case of Washington, after reviewing the various ranges available, WWU reportedly decided to build its own cyber range rather than go with Michigan's merit or other commercial programs. According to WWU's program director, they looked at other educational cyber ranges and did not feel they were necessarily appropriate, pointing out that

"Virginia and Maryland have very good programs, but those east coast programs tend to focus on government programs" whereas in Washington, they seemingly did not have a huge government presence and needed to be more focused on industry and infrastructure. (*Id*.)

Indeed, according to an EdScoop article, "cyber ranges are all the rage" in the education space as universities work to explore the most effective paths for students to join the ranks of cybersecurity professionals. "For many, cyber ranges seem to be the answer. The specially equipped computer labs or virtual centers provide test environments for users to explore and practice cybersecurity scenarios and skills, often providing certification and hands-on experience that [cannot] be practiced efficiently outside of a controlled environment." (Johnston.) As of February 2018, many other university-connected ranges have popped up across the country:

- Augusta University: Situated on the Augusta University campus, the second phase of construction for the Hull McKnight Georgia Cyber Center for Innovation and Training began in early January of this year. […] [Upon completion,] Augusta will have established one of the largest cyber training facilities in the United States. At about 330,000 square feet, the center – which is being constructed by the Georgia Technology Authority and is a partnership between multiple state and local agencies, universities and businesses – will be available to academic, industry and government officials. An on-site training ground will be available for Augusta students pursuing degrees in cybersecurity-related programs, such as information technology, computer science and intelligence and security.

- University of Central Arkansas: A $500,000 grant from the Arkansas Department of Higher Education will provide for the University of Central Arkansas to develop the state's first cyber range for students. The range will operate as the first "educational" cyber range in the region, with curricula for K-12 and higher ed[ucation] students available. […]

- Regent University: Regent University, one of the few private institutions in the country with a cyber range, opened its 3,000-square-foot facility in Virginia Beach in October 2017. The range, built with Cyberbit technology, will primarily train cybersecurity professionals and industry teams, but the university plans to dedicate at least 25 percent of the facility to undergraduate and graduate programs at Regent. […]

- University of West Florida: The University of West Florida's Center for Cybersecurity, in partnership with cyber simulations company Metova CyberCents, is currently building a cyber range open to industry, government and academic partners. The range, according to the website, will provide tests for "ethical hacking and penetration testing, computer and network security, critical infrastructure and industrial control systems security, Internet of Things security, defensive cyberspace operations and cyber war gaming." It's set to launch in October 2018.

- Grand Canyon University: The for-profit Grand Canyon University partnered with nonprofit Arizona Cyber Warfare Range, or AZCWR, to open up a cyber range on GCU's campus in the Phoenix area in November 2017. The 4,500-square-foot center is AZCWR's second and is free to the public. […] (*Id*.)

Staff notes that the list above is not exhaustive, but is illustrative of the potential cyber ranges from which California can draw to develop a cyber range appropriate for the unique needs of this state and its students. While this bill specifically names the Virginia cyber range as an example of cloud technology that could be adapted for purposes of a California cyber range, it leaves the flexibility for the pilot project to examine any other programs that already exist.

6) **Examining and potentially building on what other states such as Virginia have already developed to establish a California-specific cyber range**: This bill seeks to have up to three CSU or UC campuses host the California Cyber Range Pilot Project and require them to establish a cloud-hosted exercise area environment for hands-on cybersecurity labs and exercises for pupils and students. In doing so, the bill authorizes this effort to adapt cyber range cloud technology adopted in other states, such as Virginia, to serve typical state educational scenarios in a statewide format. Ultimately, the bill requires that the pilot project produce a scalable model for a permanent California Cyber Range Program with representative curriculum and analysis for establishing curricular enhancements and required operating expenses necessary for a statewide rollout of the cyber range. As reflected in this bill's findings and declarations, the potential utility of the cyber range is extensive:

   - The security of public and private networks is of high importance for the continued stability and prosperity of the state's economy.

   - There is a need to increase the variety and number of educational opportunities related to cybersecurity to ensure current and future workforce availability in cybersecurity roles.

   - Educational systems have been tasked to produce more graduates in cybersecurity, with demand far outpacing the ability to deliver.

   In a state that has placed increased emphasis in recent years on engaging students in topics such as computer science as part of its basic curriculum and to actively promote career development in areas such as information technology and cybersecurity, the potential benefits to schools and students cannot be overstated. For example, one of the many computer science-related bills before the Legislature for consideration this year, AB 20 (Berman), reflects the following findings and declarations, among other things: (1) providing access to computer science education is a critical step for ensuring that the state remains competitive in the global economy and strengthens its cybersecurity; (2) the outlook for computer science jobs is bright, with over 500,000 open computing positions across the country; (3) participation in high-quality computer science activities exposes pupils to the rich opportunities the field offers; (4) computing occupations make up two-thirds of all projected new jobs in the science, technology, engineering, and mathematics (STEM) fields, making computer science one of the most in-demand college majors; and, (5) the field of computer science has significant equity barriers to address, including attracting more participation by young women and underrepresented minorities to all levels and branches. (*See e.g.,* Comments 9 and 10 on prior and pending legislation.)

   The investment into and development of the cyber range reflects the value placed on such principles and could greatly help address educational, workforce, and security issues. Indeed, under this lens, the foreseeable benefits are rather significant in the long term and apply not only to students, but to all public institutions and employees as well. As discussed above, while the primary focus of the pilot project is educational, student uses in the

immediate future, the longer term vision allows for this project to be expanded into a statewide program. In doing so, this program could operate much like Virginia's, where the range is open not just to students in public educational institutions, but also any public agencies for use by public employees – be they teachers seeking credentialing, school administrators and teachers who need training on how to better protect against cyber attacks to protect educational and employee data, or public employees who wish to learn and improve upon skills necessary to their field or intended field.

Ultimately, by creating a cloud-based, safe range environment wherein student and employee users can create or recreate of cyber events and practice how to defend against them without the concern of damaging live systems or divulging real data, a cyber range can allow students, as well as current (and potentially future) public employees both inside and out of the IT, information security, and cybersecurity realm, to learn relevant curriculum, as well as receive hands on training, from wherever they happen to be. In other words, by creating a virtual sandbox "on demand," they can play (*i.e.*, train) anywhere, at any time, without any need for a formal, stationary computer lab or any added travel costs and expenses associated with securing appropriate private facilities with the necessary infrastructure. This includes the most rural of districts (with broadband access), regardless of how big or small the school's budget might be for computer labs or STEM-related activities. As long as there is a computer or tablet available with internet access, the cloud environment could be accessed with relative ease. This can open a new line of career opportunities for children all across California. In doing so, the benefits of the Cyber Range can extend to addressing other problems faced by this state, such as workforce development. As noted in a February 2018 State Scoop article, "[w]ith facilities now in various stages of completion in Arizona, Arkansas, Florida, Michigan, Virginia and Georgia, cyber ranges are quickly becoming a mainstay in government's strategy for competing with the public sector for talent and filling a widening workforce gap." (Wood, *Cyber ranges are bolstering the workforce in these six states* (Feb. 26, 2018) <https://statescoop.com/cyber-ranges-are-bolstering-the-workforce-in-these-five-states/> [as of Apr. 3, 2019].)

Lastly, while the Cyber Range is to be publicly-funded and therefore should present no cost to its public sector users, staff notes that there is the potential to open the range to private educational institutions in the future to potentially recoup some costs.

7) **California Cybersecurity Institute (CCI) to administer the program**: According to its website, the CCI, is a novel partnership among academia, industry and government. As an extension of Cal Poly's Cybersecurity Center, the CCI "aims to educate the next generation cyber workforce and provide faculty and students with a new, hands-on research and learning environment. The CCI serves as an extended Learn by Doing space for Cal Poly students to explore new cyber technologies and train and test tactics side by side with law enforcement professionals and cyberforensics experts. The program helps shape California's cyber standards and practices by offering an environment for cyberdefense innovation through advanced study and basic and applied research on emerging issues and technical challenges." (Cal Poly CCI, *About the CCI* <https://cci.calpoly.edu/about> [as of Apr. 3, 2019].)

Over the last several years, the Governor's Office of Business and Economic Development (GO-Biz) has selected Cal Poly and the California Cyber Training Complex at Cal Poly to host the CCI's Cyber Innovation Challenge. That challenge brings together participating high schools in California to compete in a state-level cybersecurity championship designed to

introduce more students to cybersecurity as a future course of study and career. The competition provides a real demonstration of the value in generating interest in and expanding access to career fields such as information technology, cybersecurity, and digital forensics, and highlights the state's young leaders in these areas. The training complex at Cal Poly is a100,000 square foot state-of-the-art training and lecture facility that emphasizes hands on cybersecurity and cyber forensics training, aimed at developing next-generation cyber forensics techniques and tactics. By naming CCI as the entity with responsibility for administering the pilot project, this bill would draw on the expertise already developed at CCI and the training complex at Cal Poly. At the same time, the bill leaves open the opportunity for other CSUs and UCs to participate in hosting the project.

8) **Possible reporting requirement**: As noted in Comment 10, below, this bill is double-referred to the Assembly Higher Education Committee. If this Committee approves this bill, the author may wish to consider an amendment in that committee to add a reporting requirement that would, at minimum, provide updates on the development of this cyber range project, and the plan for statewide rollout, to the California Department of Technology and this Committee. This would also add sufficient time to allow the other committee to consider other entities or policy committees it deems appropriate for reporting purposes.

9) **Related legislation**: AB 20 (Berman) *See* Comment 6.

10) **Prior legislation**: SB 436 (Allen, 2017) would have established the California STEM Professional Teaching Pathway to recruit, train, support, and retain qualified STEM professionals, including military veterans, as mathematics and science teachers in California, upon an appropriation being included in the annual Budget Act. This bill was held in Assembly Education Committee.

    AB 2329 (Bonilla, Ch. 693, Stats. 2016) required the Superintendent of Public Instruction to convene a computer science strategic implementation advisory panel to develop recommendations for a computer science strategic implementation plan.

    AB 1539 (Hagman Ch. 876, Stats. 2014) required the Instructional Quality Commission and the State Board of Education to consider developing computer science content standards.

11) **Double-referral**: This bill is double-referred to the Assembly Higher Education Committee, where it will be heard if approved by this Committee.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

Analysis Prepared by: Ronak Daylami / P. & C.P. / (916) 319-2200