Date of Hearing: April 23, 2019

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 1242 (Irwin) – As Amended April 12, 2019

SUBJECT: Office of Cybersecurity

SUMMARY: This bill would establish, in the Governor's office, the Office of Cybersecurity under the direction of a new Director of the Office of Cybersecurity. The bill would make the Office of Cybersecurity (Office) responsible for, among other things, advising the Governor on issues of information security, privacy, and cybersecurity and would transfer the duty of establishing and leading the California Cybersecurity Integration Center (Cal-CSIC) from the California Office of Emergency Services (Cal OES) to the Office. This bill would also clarify that all state agencies, as defined under existing law, must comply with the policies and procedures of the Office of Information Security (OIS) within the California Department of Technology (CDT), and not simply those state entities under the direct authority of the Governor. Among other things, this bill would require OIS to consult with the Office when establishing the information security program and transfer specified duties related to information security assessments (ISAs) and audits from OIS to the Office. Specifically, **this bill would**:

1) Replace Cal OES as the lead of Cal-CSIC with the Office, with the authority to add other members to the statutorily prescribed membership of Cal-CSIC, and would add representatives of the Office to Cal-CSIC's membership.

2) Specify that Cal-CSIC must operate not only in close coordination with the Cal State Threat Assessment System and the United States Department of Homeland Security – National Cybersecurity and Communications Integration Center as otherwise required under existing law, but also in close coordination with Cal OES.

3) Replace a variety of references to "state agency" and "state entity" in the statutes governing OIS with a specific reference to "state agency" that is defined under existing law to mean every state office, officer, department, division, bureau, board, and commission, except for the California State University. In doing so, this bill would require all state agencies, in this broader understanding of the term, to implement OIS-issued policies and procedures, and not just those state entities under the direct authority of the Governor.

4) Revise the responsibility of the OIS chief to establish an information security program to require the chief to do so in consultation with the Office. This bill would revise the program responsibilities to:

    - Require the consultation of the Office in representing the State before the federal government, other state agencies, local government entities, and private industry on issues that have statewide impact on information security and privacy.

    - Add a new responsibility for, in consultation with the Office, the creation and operation of select centralized security services, including, but not limited to the CDT Security Operations Center (SOC).

5) Repeal OIS's authority to conduct, or require to be conducted, an ISA of every state agency, department, or office.

6) Require OIS, in consultation with the Office (as opposed to Cal OES), to perform ISAs as otherwise specified under existing law.

7) Repeal OIS's authority to conduct or require to be conducted an audit of information security to ensure program compliance.

8) Repeal an existing requirement for OIS report to CDT and Cal OES any state entity found to be noncompliant with information security program requirements. This bill would also repeal the responsibility of OIS to report to Cal OES, the Department of California Highway Patrol (CHP) and the Department of Justice regarding any criminal or alleged criminal cyber activity affecting any state entity or critical infrastructure of state government.

9) Establish a new Office of Cybersecurity in the office of the Governor to advise the Governor on information security, privacy, and the cybersecurity posture of the State and to lead and coordinate the State's day to day response to cybersecurity incidents, as well as statewide information security, privacy and cybersecurity initiatives.

10) Provide that the Governor must appoint the Director of Cybersecurity to serve at the pleasure of the Governor and lead the Office in carrying out its powers and duties.

11) Specify that the Office, under the direction of the director, must perform all of the following duties, among other things:

    - Serve as chief advisor to the Governor on matters pertaining to information security, privacy, and cybersecurity.

    - Serve as lead coordinator for nonemergency response to the breach or attempted breach of the confidentiality, integrity, or availability of state systems and applications, as specified, whereas Cal OES and the "State Operations Center" are to lead the response to an emergency proclaimed by the Governor related to a cybersecurity event.

    - Operate and maintain Cal-CSIC.

    - Lead private sector and education partnership efforts to build out a workforce pathway of cybersecurity expertise.

    - Have responsibility for oversight of OIS in providing strategic direction for information security and privacy to state government agencies, departments and offices, as specified.

    - Have the authority to conduct, or require to be conducted, an ISA of every state agency, department, or office, as specified.

    - Act as the State's Chief Information Security Officer (CISO) representative as specified, and represent the State before the federal government, other state agencies, local government entities, and private industry on issues that have statewide impact on cybersecurity.

- Notify Cal OES, CHP, OIS, and DOJ regarding any criminal or alleged criminal cyber activity affecting any state entity or critical infrastructure of state government.

12) Make other conforming changes.

EXISTING LAW:

1) Establishes 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).)

2) Establishes OIS within CDT to ensure the confidentiality, integrity, and availability of state systems and applications. OIS is under the direction of a chief, appointed by and serving at the pleasure of the governor, to lead OIS in carrying out its mission. The Chief must report to the director of CDT and the duties of OIS under the Chief's direction are to provide direction for information security and privacy to state government agencies, departments, and offices, as specified further, below. Generally speaking, requires OIS to develop an information security program and establish policies, standards, and procedures directing state agencies to effectively manage security and risk. (Gov. Code Sec. 11549 et seq.)

3) Requires all state entities defined below to implement the policies and procedures issued by OIS, including, but not limited to, performing both of the following duties:

   - Comply with the information security and privacy policies, standards, and procedures issued by OIS.

   - Comply with filing requirements and incident notification by providing timely information and reports as required by OIS. (Gov. Code Sec. 11549.3(b).)

4) Defines "state entity" for purposes of the above provision and a separate provision requiring state agencies and entities to have chief information officers and information security officers, only, to mean an entity within the executive branch that is under the direct authority of the Governor. This includes, but is not limited to, all departments, boards, bureaus, commissions, councils, and offices that are not defined as a "state agency." In turn, "state agency" means the Transportation Agency, Department of Corrections and Rehabilitation, Department of Veterans Affairs, Business, Consumer Services, and Housing Agency, Natural Resources Agency, California Health and Human Services Agency, California Environmental Protection Agency, Labor and Workforce Development Agency, and Department of Food and Agriculture. (Gov. Code Sec. 11546.1.)

5) Authorizes OIS to conduct, or require to be conducted, an ISA of every state agency, department, or office. (Gov. Code Sec. 11549.3(c)(1).)

6) Requires OIS to perform specified duties in consultation with Cal OES, including annually requiring no fewer than 35 state entities to perform an ISA, the cost of which shall be funded by the state agency, department, or office being assessed. (Gov. Code Sec. 11549.3(c)(2).)

7) Authorizes the California Military Department (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).)

8) Requires state agencies and entities that are required to conduct or receive an ISA 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(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).)

9) Requires Cal OES to establish and lead the Cal-CSIC, the primary mission of which 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. Cal-CSIC serves 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, academic institutions, and nongovernmental organizations. (Gov. Code Sec. 8586.5(a).)

10) Specifies that Cal-CSIC must be comprised of representatives from the following organizations, among others: Cal OES; OIS; the State Threat Assessment Center; CHP; CMD; U.S. Department of Homeland Security; U.S. Federal Bureau of Investigation; U.S. Secret Service; U.S. Coast Guard; and other members as designated by the Cal OES director. (Gov. Code Sec. 8586.5(a).)

11) Requires 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, private companies, and other appropriate sources. Cal-CSIC must provide warnings of cyber attacks 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. (Gov. Code Sec. 8586.5(b).)

12) Requires Cal-CSIC to also do the following:

    - 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. The cybersecurity strategy must: (1) be developed to improve how cyber threats are identified, understood, and shared in order to reduce threats to California government, businesses, and consumers; and, (2) also 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.

- 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. This team shall also assist law enforcement agencies with primary jurisdiction for cyber-related criminal investigations and agencies responsible for advancing information security within state government. (Gov. Code Sec. 8586.5(c)-(d).)

13) Provides, under Section 11000 of the Government Code, that as used in that title on the Government of the State of California, which also governs CDT and OIS, "state agency" includes every state office, officer, department, division, bureau, board, and commission. "State agency" does not include the California State University unless the section explicitly provides that it applies to the university. (Gov. Code Sec. 11000(a).)

14) Provides under the cybersecurity article of the Emergency Services Act of the Government Code, that "state agency" or "state agencies" means the same as "state agency" as set forth in Section 11000, above. (Gov. Code Sec. 8592.30(f).) Requires under this article that CDT, in consultation with Cal OES and compliance with Section 11549.3, above, update the Technology Recovery Plan element of the State Administrative Manual (SAM) to ensure the inclusion of cybersecurity strategy incident response standards for each state agency to secure its critical infrastructure controls and critical infrastructure information. (Gov. Code Sec. 8592.35(a)(1).)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of this bill**: This bill seeks to establish an Office of Cybersecurity in the Office of the Governor and transfer various responsibilities and duties of Cal OES and CDT's OIS to the Office, with oversight of OIS to be moved from CDT's director to the director of the new Office, as well. This is an author-sponsored bill.

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

> The current reporting structure to the Governor on cybersecurity issues is fragmented, and in many instances is structured to create numerous intermediaries between the expert and the Governor. Some of these intermediaries are also charged with advising the Governor on topics that conflict directly or indirectly with cybersecurity, or compete for resources.
>
> The elevation of direct cybersecurity advice to the key decision maker has been a trend in the private sector with direct access for CISO's to the CEO or Board of Directors a new best practice. […]
>
> At the federal level there have been various shifts in the placement of cybersecurity coordination dating back to the George W. Bush Administration.
>
> []The first "cyber czar" fell within the Office of Management and Budget; the "czar" job shifted to the Department of Homeland Security, with the formation of the National Cybersecurity Center and Rod Beckstrom serving as its first director. But while DHS took over oversight of cybersecurity for the civilian agencies of government, there was

still no single point of guidance for coordinating policy and security operations across all the government's networks. Beckstrom resigned from the job because of a lack of funding—and a lack of cooperation from the NSA.

That problem led to the creation of the National Cybersecurity Coordinator role—one czar to rule all the cyber—as part of the National Security Council. […] These shifts culminated in a "Cybersecurity Coordinator" position in the White House, as an Assistant to the President […].

However in 2018, the Trump Administration eliminated the role when John Bolton became National Security Advisor, with many new reports asserting that Bolton wanted to limit "competitive power centers emerging inside the national security apparatus" and that "Cybersecurity experts and members of Congress said they were mystified by the move" […]

Currently California's state government cybersecurity efforts are a coordinated effort among the "core four", CDT, OES, CMD, and CHP.

The bulk of planning, standards, and coordination of day-to-day information security are under the purview of CDT, specifically the OIS, which is in charge of SAM and SIMM [Statewide Information Management Manual] provisions related to information security and oversees the Audit and Independent Security Assessment programs. OIS also has a Security Operations Center, which monitors the Statewide Network (C-GEN) including network traffic to the State Data Center and pass through network traffic to cloud services providers. CDT also provides project planning and oversight for large-scale IT projects, allowing them to assist in the information security planning of state IT programs. The director of OIS, the state CISO, must report cybersecurity problems through the Director of CDT, the CIO, who then must report to the Secretary of Government Operations, who as a cabinet-level official may directly advise the Governor. The Director of CDT/CIO is also charged with oversight of the State's IT infrastructure, IT project planning and delivery, and overall IT spending.

AB 1242, creates a new Office of Cybersecurity within the Office of the Governor, and re-organizes certain duties that are currently under other state entities to the new Office. It specifically:

> Creates the Office of Cybersecurity, and designates the Director of the office to be the chief advisor to the Governor on cybersecurity.
>
> Places the Office of Cybersecurity as the lead of the Cal-CSIC, replacing the Office of Emergency Services[.]
>
> Places the Office of Cybersecurity as the lead for Information Security Audits and Independent Security Assessments (ISAs), replacing OIS[.]
>
> Requires the Chief of the Office of Information Security (OIS) within CDT to consult with the Office of Cybersecurity in carrying out OIS duties.

The bill also changes the statutory references to state entities under Section 11546.1 to state agency under section 11000, which will have the effect of bringing state agencies

that do not directly report to the Governor under the policy, reporting, and compliance authority of OIS's information security directives.

3) **Restructuring the State's cybersecurity leadership approach**: Last year, this Committee and the Select Committee on Cybersecurity (chaired by the author of this bill) held a joint oversight hearing on the topic of Cybersecurity. As discussed in that hearing, the four core partners in cybersecurity, Cal OES, CDT (including OIS), CMD, and CHP, have been working effectively together to better secure the cybersecurity posture of the State. This coordinated partnership approach represents a critical shift away from a generally siloed approach by state agencies and departments to cybersecurity issues, which had proven inefficient and less effective. Indeed, in 2015 and 2016, the committees held hearings on the same topic wherein systemic inadequacies at the leadership level and throughout California's information technology enterprise related to cybersecurity were uncovered. (*See* joint hearings of this Committee and the Assembly Cybersecurity Select Committee held on April 6, 2015, entitled "Cybersecurity at the State-Level" and February 24, 2016, entitled "Assessing California's Cybersecurity Strategy: Is the State Prepared to Defend Itself Against 21st Century Attacks?") In the interceding three years between those earlier hearings and the 2018 hearing, both the Executive Branch and the Legislature undertook many efforts to bolster the cybersecurity posture of the State, including the development of Cal-CSIC pursuant to an executive order that was codified last year in light of its efficacy. (*See* AB 2813 (Irwin, Ch. 768, Stats. 2018).) Effectively, the oversight hearing in 2018 demonstrated that cybersecurity threats are on the rise, but so too is the State's effectiveness[1] in combatting those threats due to consistent policies, changes in technologies, coordination among departments led by these entities, information sharing and resource pooling, among other things.

   For the most part, this bill, notably, arises out of concern that this State's reporting to the Governor is fragmented – as opposed to a concern that the State's approach to cybersecurity defense itself remains fragmented or siloed. (There is one exception to this, further discussed in Comment 4). Despite the fact that Cal OES and CDT serve at the pleasure of the Governor and report directly to the Governor, and the working partnership between these entities and CMD and CHP, this bill seeks to introduce a new Office of Cybersecurity within the Governor's Office and shift many of Cal OES' current responsibilities and duties for Cal-CSIC and CDT/OIS's information security program and policies (including ISAs and audits) to that Office. This bill would also require oversight over OIS by the new Office, and potentially interfere with the oversight of OIS by the CDT director. If decisions were made that prove unsound or negligent, it is unclear that the director of this new Office would, or could, be held accountable by the Legislature, as opposed to the director of CDT who is Senate confirmable and whose department is subject to regular oversight hearings by this Committee.

---

[1] This is not to suggest that all state departments and agencies are prioritizing and approaching cybersecurity the right way, or with the diligence it requires; just that the four leaders on cybersecurity for the state have made impressive achievements in working together to get departments and agencies on the right path and to respond to issues when they arise. This is an important distinction, as the subject of this bill is, in fact, on the leadership of two of the four core partners – not the problems that exist in departments that still lag behind their counterparts in prioritizing and following state policies and practices in cybersecurity.

Indeed, this new Office would be headed by a Governor-appointee, who would not otherwise be subject to Senate confirmation – unlike the directors of Cal OES and CDT. (*See* Gov. Code Secs. 8585.1 and 11545.)

Arguably, if the concern is that the heads of Cal OES and CDT are not reporting appropriately to the Governor's office, the Governor has the authority to remove them and appoint new directors, subject to confirmation, or otherwise institute internal processes to require joint reports if the reports are fragmented and conflicting. Alternatively, if the concern is that those directors have priorities that might not align with cybersecurity efforts of the Chief Information Security Officer (the Chief of OIS) and divert funding from that office, then perhaps the solution would be to secure a funding stream directly for that office. Absent demonstrated problems related to the partnership approach to cybersecurity in this State by these four core partners or a desire by the Governor's office to change the reporting structure of these entities, it is not apparent that this bill would help the cybersecurity posture of this State. It could, in fact, potentially hurt it, however unintentionally.

While the Assembly Governmental Organization (G.O.) Committee has oversight function over Cal OES, this Committee oversees CDT and is unaware of cases warranting the proposed removal of authority from OIS or the proposed transition of oversight authority over OIS from the director of CDT to this Office. If this Committee were to approve this bill, it may wish to seek an agreement from the author to strike all sections of this bill relating to CDT's OIS, except for one limited change in Section 3 (Gov. Code Sec. 11549.3(b)) discussed further below. Due to procedural issues and the double-referral to the Assembly G.O. Committee, any amendments committed to by the author or requested by this Committee should be processed before this bill is taken up in the *Appropriations* Committee – thereby allowing Assembly G.O. to hear the bill in its current form and consider issues specific to that committee.

4) **Requiring all state agencies, and not just state entities, to follow OIS' policies and procedures**: Under existing law, in the Government Code, unless a specific definition is given otherwise, the default definition for "state agency" includes every state office, officer, department, division, bureau, board, and commission, except the CSUs. By and large, provisions pertaining to CDT use the term "state agency" without providing a specific definition, and thus the default definition of Section 11000 applies in those situations. In various other provisions relating to CDT (including OIS), however, the term "state entity" appears, largely without a correlating definition. In two instances, only, (first, a provision requiring state agencies and entities to have chief information officers and information security officers; and, second, a provision requiring state entities to comply with OIS policies and procedures) the term "state entity" is specifically defined mean an entity within the executive branch that is under the direct authority of the Governor, including, but not limited to, all departments, boards, bureaus, commissions, councils, and offices *that are not defined as a "state agency."* (Gov. Code Sec. 11546.1(e)(2).) For this purpose, "state agency" means the Transportation Agency, Department of Corrections and Rehabilitation, Department of Veterans Affairs, Business, Consumer Services, and Housing Agency, Natural Resources Agency, California Health and Human Services Agency, California Environmental Protection Agency, Labor and Workforce Development Agency, and Department of Food and Agriculture. (Gov. Code Sec. 11546.1(e)(1).)

The lack of consistency in terminology around state agencies and state entities has created a critical discrepancy between the responsibilities that this Legislature has assigned to CDT, and particularly OIS, and the ability of those offices to execute the duties the Legislature requires them to execute.

Namely, in the primary statute delineating OIS' responsibilities, OIS must develop an information security program and, among other things, establish policies, standards, and procedures directing *state agencies* to effectively manage security and risk. (*See* Gov. Code Sec. 11549.3(a)(2).) In this instance, due to lack of specificity, the default definition of "state agency" under Section 11000 applies, to include every state office, officer, department, division, bureau, board, and commission.

In the very next subdivision of this same statute pertaining to OIS' responsibilities, however, it then states that "all *state entities defined in Section 11546.1*" must comply with those information security policies, standards and procedures. (*See* Gov. Code Sec. 11549.3(b).) Accordingly, only those executive branch entities with direct reporting to the Governor that are not the state agencies enumerated, above, need comply. As a result, independent constitutional offices in the executive branch do not have to comply with information security policies, standards, and procedures that otherwise apply to the executive branch.

Even still, in the next subdivision, enacted by way of more recent legislation (AB 670 (Irwin, Ch. 518, Stats. 2015), the terms "state agency" and "state entity" are both used in various ways in relation to OIS information security assessments related duties, in conjunction with Cal OES – though the construct of the subdivision suggests that state entity is meant to be read as an "all encompassing" term that covers not only state agencies, but also offices and departments. Specifically, that subdivision states that OIS may conduct, or require to be conducted, an independent security assessment of *every state agency, department, or office*, and then in the very next paragraph states that OIS, in consultation with Cal OES must annually require no fewer than 35 *state entities* to perform an independent security assessment, the cost of which shall be funded by the *state agency, department, or office* being assessed. (*Compare* Gov. Code Sec. 11549.3(c)(1) to Gov. Code Sec. 11549.3(c)(2)(A).)

While the term "state entity" in that subdivision does not rely on the same narrow definition in Section 11546.1 as the previous subdivision does, it has led to much confusion over OIS's authority to conduct ISAs of offices in the Executive Branch, not all of whom report directly to the Governor.

This bill would remove any ambiguity, by clearly stating that all state agencies defined in Section 11000 of the Government Code must comply with OIS' policies and procedures moving forward. This would be consistent with all other provisions in CDT's chapter in the Government Code and other articles relating to CDT which similarly rely on that Section 11000 definition. As a result, the only instance in which the narrow "state entity" definition would remain would be in Section 11546.1, which sets forth the state agencies (cabinet agencies) and state entities (those with direct reporting to the Governor) that must have a CIO and information security officer within their organization.

This would help ensure that the four core partners with jurisdiction over cybersecurity, CDT, Cal OES, CMD and CHP, have the best visibility into all state agencies, offices, and

departments. Staff notes that in this particular section of the bill, this bill is identical to AB 3193 (Chau et al.), which this Committee approved unanimously just last year.

In opposition, the Betty Yee, the State Controller, writes:

> This measure is similar in concept to – though significantly broader and more intrusive than – AB 3193 (Chau), which was defeated in the Senate Governmental Organization Committee just last year.
>
> […] Giving CDT and OC [Office of Cybersecurity] this unprecedented level of control over SCO means that I will not be able to effectively prioritize my programs and control my budget. SCO is a separate, independent constitutional office. it is not, contrary to the policies proposed in AB 1242, a department under any gubernatorial administration.
>
> Nine years ago, AB 2408 (Smyth), Chapter 404, Statutes of 2019, was enacted to codify the Governor's Reorganization Plan No. 1 of 2009. Provisions to place the constitutional offices under the jurisdiction of CDT were remove din favor of a requirement that constitutional offices voluntarily comply with the requirements set forth in the Reorganization Plan.
>
> Since AB 2408 was enacted in 2010, SCO has lived up to the commitment to meet or exceed the standards established by that law. As a result, I do not see what problem AB 1242 seeks to solve. […] If there is something that is not working in statute or in practice, I am committed to discussing how to quickly address it. However, the reach of AB 1242 is too broad, the powers it hands to CDT and OC are unprecedented, and the manner in which it impinges on all of California's statewide constitutional offices is unacceptable.

5) **Prior Legislation**: AB 3193 (Chau et al, 2018) would have clarified that all state agencies, as defined under existing law, must comply with the policies and procedures of CDT's OIS, and not simply those state entities under the direct authority of the Governor. That bill died in the Senate Governmental Organization Committee.

6) **Double-referral**: This bill is double-referred to the Assembly G.O. Committee.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

State Controller, Betty Yee

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