AMENDED IN SENATE AUGUST 15, 2016

AMENDED IN SENATE AUGUST 2, 2016

AMENDED IN ASSEMBLY APRIL 14, 2016

AMENDED IN ASSEMBLY MARCH 28, 2016

CALIFORNIA LEGISLATURE—2015–16 REGULAR SESSION

ASSEMBLY BILL No. 1841

Introduced by Assembly Member Irwin
(Coauthor: Senator Jackson)

February 9, 2016

An act to add Article 6.4 (commencing with Section 8592.30) to Chapter 7 of Division 1 of Title 2 of the Government Code, relating to state government.

LEGISLATIVE COUNSEL'S DIGEST

AB 1841, as amended, Irwin. Cybersecurity *strategy* incident response ~~plan and~~ standards.

(1) The California Emergency Services Act sets forth the duties of the Office of Emergency Services with respect to specified emergency preparedness, mitigation, and response activities within the state. Existing law establishes the Department of Technology under the supervision of the Director of Technology who is also known as the State Chief Information Officer, and generally requires the Department of Technology to be responsible for the approval and oversight of information technology projects by, among other things, consulting with state agencies during initial project planning to ensure that project proposals are based on well-defined programmatic needs. *Existing law establishes the Office of Information Security, within the Department*

of Technology, under the direction of a chief who reports to the Director of Technology.

This bill would require the ~~Office of Emergency Services, in conjunction with the Department of Technology, to transmit to the Legislature, on or before July 1, 2017, a cybersecurity incident response plan, known as the Cyber Security Annex to the State Emergency Plan, Emergency Function 18, or EF 18. The bill would further require the office, in conjunction with the Department of Technology and on or before January 1, 2018, to develop cybersecurity incident response standards for state agencies, as defined, to, among other things, prepare for cybersecurity interference with, or the compromise or incapacitation of, critical infrastructure and would require state agencies to report their compliance with these standards to the office.~~ *Department of Technology, in consultation with the Office of Emergency Services and compliance with the information security program required to be established by the chief of the Office of Information Security, to update the Technology Recovery Plan element of the State Administrative Manual to ensure the inclusion of cybersecurity strategy incident response standards for each state agency to secure its critical infrastructure controls and critical infrastructure information.* The bill would require ~~the office, in conjunction with the Department of Technology,~~ *each state agency to provide its updated Technology Recovery Plan and report on its compliance with these updated standards to the department, as specified, and authorize the department, in consultation with the Office of Emergency Services,* to provide suggestions for a state agency to improve compliance with these standards. *The bill would define terms for its purposes and make legislative findings in support of its provisions.* The bill would prohibit public disclosure of reports and public records relating to the cybersecurity strategies of state agencies, as specified.

(2) Existing constitutional provisions require that a statute that limits the right of access to the meetings of public bodies or the writings of public officials and agencies be adopted with findings demonstrating the interest protected by the limitation and the need for protecting that interest.

This bill would make legislative findings to that effect.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. The Legislature finds and declares all the following:

(a) The current pervasive use of information technology in public enterprises has resulted in an abundance of public access to information and services provided by the government, but the increased interdependence of information technology systems has created a new type of risk for society. Threats to public critical infrastructure that use information technology within the state present risks to public health and safety and could severely disrupt economic activity within California.

(b) Ensuring sufficient preparations are taken to protect critical infrastructure from interference, compromise, or incapacitation are in the public interest and serve a public purpose.

(c) A comprehensive cybersecurity ~~incident response plan, undertaken~~ *strategy, related to state agency critical infrastructure information and control, developed* in a coordinated effort among state agencies, will help prepare for threats to critical infrastructure, thereby reducing the potential consequences from those attacks.

(d) The Department of Technology, in its role as the lead entity that coordinates state resources in the development of information technology (IT) strategy and policy, directs state agency information security and privacy standards and procedures for the day-to-day protection of state information assets from a variety of threats, including, but not limited to, cybersecurity threats and attacks.

~~(d)~~

(e) The Office of Emergency Services, in its role as the lead executive entity that coordinates state resources for emergency preparedness, response, and damage mitigation, is ~~a state entity appropriate to develop, implement, and manage a comprehensive cybersecurity incident response plan, undertaken in a coordinated effort among state agencies, to protect critical infrastructure. The Office of Emergency Services is already developing the necessary expertise in cybersecurity through its current work developing methods to provide emergency services during an interference with, or the compromise or incapacitation of, critical infrastructure.~~ *integrating cybersecurity into the State Emergency Plan.*

(f) The Department of Technology is continuing its state government oversight and compliance monitoring program, and enhancing day-to-day information security incident response coordination with the Office of Emergency Services, Department of the California Highway Patrol's Computer Crimes Investigation Unit, and the Military Department.

~~(e)~~

(g) It is the intent of the Legislature in enacting this legislation to ~~develop a~~ *add to the ongoing work of the state's* comprehensive cybersecurity ~~incident response plan,~~ *strategy,* undertaken in a coordinated effort among state agencies, to prepare California for threats to critical infrastructure under the unifying coordination of the Office of Emergency Services.

SEC. 2. Article 6.4 (commencing with Section 8592.30) is added to Chapter 7 of Division 1 of Title 2 of the Government Code, to read:

Article 6.4. Cybersecurity

8592.30. As used in this article, the following definitions shall apply:

(a) "Critical ~~infrastructure"~~ *infrastructure controls"* means *networks and* systems ~~and~~ *controlling* assets so vital to the state that the incapacity or destruction of those ~~systems~~ *networks, systems,* or assets would have a debilitating impact on ~~security, economic security, public health and safety, or any combination of those matters.~~ *public health, safety, economic security, or any combination thereof.*

(b) "Critical infrastructure information" means information not customarily in the public domain pertaining to any of the following:

(1) Actual, potential, or threatened interference with, or an attack on, compromise of, or incapacitation of critical infrastructure *controls* by either physical or computer-based attack or other similar conduct, including, but not limited to, the misuse of, or unauthorized access to, all types of communications and data transmission systems, that violates federal, state, or local ~~law, harms economic security, or threatens public health or safety.~~ *law or harms public health, safety, or economic security, or any combination thereof.*

(2) The ability of critical infrastructure *controls* to resist any interference, compromise, or incapacitation, including, but not limited to, any planned or past assessment or estimate of the vulnerability of critical ~~infrastructure, including, but not limited to, security testing, risk evaluation, risk management planning, or risk audits.~~ *infrastructure.*

(3) Any planned or past operational problem or solution regarding critical ~~infrastructure,~~ *infrastructure controls,* including, but not limited to, repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to interference, compromise, or incapacitation of critical ~~infrastructure.~~ *infrastructure controls.*

(c) "Department" means the Department of Technology.

(d) "Office" means the Office of Emergency Services.

~~(c)~~

(e) "Secretary" means the secretary of each state agency as set forth in subdivision (a) of Section 12800.

~~(d)~~

(f) "State agency" or "state agencies" means the same as "state agency" as set forth in Section 11000.

~~8592.35. (a) On or before July 1, 2017, the office, in conjunction with the Department of Technology, shall transmit to the Legislature a cybersecurity incident response plan, known as the Cyber Security Annex to the State Emergency Plan Emergency Function 18, or EF 18, that includes, but is not limited to, all of the following:~~

~~(1) Methods for providing emergency services.~~

~~(2) Command structure for statewide coordinated emergency services.~~

~~(3) Emergency service roles of appropriate state agencies.~~

~~(4) Identification of resources to be mobilized.~~

~~(5) Public information plans.~~

~~(6) Continuity of government services.~~

~~(b) The office shall transmit the plan to the Legislature pursuant to Section 9795.~~

~~8592.40.~~

8592.35. (a) (1) On or before ~~January~~ *July* 1, 2018, ~~in conjunction with the Department of Technology, the office shall develop cybersecurity incident response standards for state agencies to prepare for cybersecurity interference with, or the compromise or incapacitation of, critical infrastructure and the development of~~

~~critical infrastructure information, and to transmit critical infrastructure information to the office. In developing the standards, the office shall consider all of the following:~~ *the department shall, in consultation with the office and compliance with Section 11549.3, update the Technology Recovery Plan element of the State Administrative Manual to ensure the inclusion of cybersecurity strategy incident response standards for each state agency to secure its critical infrastructure controls and critical infrastructure information.*

(2) In updating the standards in paragraph (1), the department shall consider, but not be limited to considering, all of the following:

~~(a)~~

(A) Costs to implement the standards.

~~(b)~~

(B) Security of critical infrastructure information.

~~(c)~~

(C) Centralized management of risk.

~~(d)~~

(D) Industry best practices.

~~(e)~~

(E) Continuity of operations.

~~(f)~~

(F) Protection of personal information.

(b) Each state agency shall provide the department with a copy of its updated Technology Recovery Plan.

~~8592.45.~~

8592.40. (a) Each state agency shall report on its compliance with the standards ~~developed~~ *updated* pursuant to Section ~~8592.40~~ *8592.35* to the ~~office~~ *department* in the manner and at the time directed by the ~~office,~~ *department,* but no later than ~~January~~ *July* 1, 2019.

(b) The ~~office,~~ *department,* in conjunction with the ~~Department of Technology, shall~~ *office, may* provide suggestions for a state agency to improve compliance with the standards developed pursuant to Section ~~8592.40,~~ *8592.35,* if any, to the head of the state agency and the secretary responsible for the state agency. For a state agency that is not under the responsibility of a secretary, the ~~office~~ *department* shall provide any suggestions to the head of the state agency and the Governor.

~~8592.50~~

8592.45. The *information required by subdivision (b) of Section 8592.35, the* report required by subdivision (a) of Section ~~8592.45~~ *8592.40,* and any public records relating to any communication made pursuant to, or in furtherance of the purposes of, subdivision (b) of Section ~~8592.45~~ *8592.40* are confidential and shall not be disclosed pursuant to any state law, including, but not limited to, the California Public Records Act (Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1).

SEC. 3. The Legislature finds and declares that Section 2 of this act, which adds Section ~~8592.50~~ *8592.45* to the Government Code, imposes a limitation on the public's right of access to the meetings of public bodies or the writings of public officials and agencies within the meaning of Section 3 of Article I of the California Constitution. Pursuant to that constitutional provision, the Legislature makes the following findings to demonstrate the interest protected by this limitation and the need for protecting that interest:

Preventing public disclosure of the individual cybersecurity preparations *and critical infrastructure information* of state agencies promotes public safety by prohibiting access to those who would use that information to thwart the cybersecurity of critical infrastructure *controls* within the state.

O