

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

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 ~~emergency services~~. *state government*.

LEGISLATIVE COUNSEL'S DIGEST

AB 1841, as amended, Irwin. ~~Office of Emergency Services: duties: cybersecurity~~. *Cybersecurity 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.*

This bill would require the Office of Emergency ~~Services~~ *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, ~~also known as Emergency Function 18~~ *18*, or EF 18. The bill would

further require the ~~office~~ *office, in conjunction with the Department of Technology and on or before January 1, 2018, to develop a comprehensive cybersecurity strategy setting 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 ~~its~~ *their* compliance with these standards to the office. The bill would require the ~~office~~ *office, in conjunction with the Department of Technology,* to provide suggestions for a state agency to improve compliance with these standards. 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:

- 1 SECTION 1. The Legislature finds and declares all the
- 2 following:
- 3 (a) The current pervasive use of information technology in
- 4 public enterprises has resulted in an abundance of public access
- 5 to information and services provided by the government, but the
- 6 increased interdependence of information technology systems has
- 7 created a new type of risk for society. Threats to public critical
- 8 infrastructure that use information technology within the state
- 9 present risks to public health and safety and could severely disrupt
- 10 economic activity within California.
- 11 (b) Ensuring sufficient preparations are taken to protect critical
- 12 infrastructure from interference, compromise, or incapacitation
- 13 are in the public interest and serve a public purpose.
- 14 (c) A comprehensive cybersecurity ~~strategy,~~ *incident response*
- 15 *plan,* undertaken in a coordinated effort ~~between~~ *among* state
- 16 agencies, will help prepare for threats to critical infrastructure,
- 17 thereby reducing the potential consequences from those attacks.

1 (d) The Office of Emergency Services, in its role as the lead
2 executive entity that coordinates state resources for emergency
3 preparedness, response, and damage mitigation, is a state entity
4 appropriate to develop, implement, and manage a comprehensive
5 cybersecurity—~~strategy~~, *incident response plan*, undertaken in a
6 coordinated effort ~~between~~ *among* state agencies, to protect critical
7 infrastructure. The Office of Emergency Services is already
8 developing the necessary expertise in cybersecurity through its
9 current work developing methods to provide emergency services
10 during an interference with, or the compromise or incapacitation
11 of, critical infrastructure.

12 (e) It is the intent of the Legislature in enacting this legislation
13 to develop a comprehensive cybersecurity—~~strategy~~, *incident*
14 *response plan*, undertaken in a coordinated effort ~~between~~ *among*
15 state agencies, to prepare California for threats to critical
16 infrastructure under the unifying coordination of the Office of
17 Emergency Services.

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

21
22 Article 6.4. Cybersecurity

23
24 8592.30. As used in this article, the following definitions shall
25 apply:

26 (a) “Critical infrastructure” means systems and assets so vital
27 to the state that the incapacity or destruction of those systems or
28 assets would have a debilitating impact on security, economic
29 security, public health and safety, or any combination of those
30 matters.

31 (b) “Critical infrastructure information” means information not
32 customarily in the public domain pertaining to any of the following:

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

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

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

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

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

15 8592.35. (a) On or before July 1, 2017, the ~~office~~ *office, in*
16 *conjunction with the Department of Technology*, shall transmit to
17 the Legislature *a cybersecurity incident response plan, known as*
18 *the Cyber Security Annex to the State Emergency Plan, also*
19 ~~known as~~ *Emergency Function 18 18, or EF 18*, that includes, but
20 is not limited to, all of the following:

- 21 (1) Methods for providing emergency services.
- 22 (2) Command structure for ~~state-wide~~ *statewide* coordinated
23 emergency services.
- 24 (3) Emergency service roles of appropriate state agencies.
- 25 (4) Identification of resources to be mobilized.
- 26 (5) Public information plans.
- 27 (6) Continuity of government services.

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

30 8592.40. ~~(a)~~ *On or before July January 1, 2018, in conjunction*
31 *with the Department of Technology*, the office shall develop ~~a~~
32 ~~comprehensive~~ *cybersecurity strategy setting incident response*
33 standards for state agencies to prepare for cybersecurity
34 interference with, or the compromise or incapacitation of, critical
35 infrastructure and the development of critical infrastructure
36 information, and to transmit critical infrastructure information to
37 the office. In developing the standards, the office shall consider
38 all of the following:

- 39 ~~(1)~~
- 40 (a) Costs to implement the standards.

- 1 ~~(2)~~
- 2 (b) Security of critical infrastructure information.
- 3 ~~(3)~~
- 4 (c) Centralized management of risk.
- 5 ~~(4)~~
- 6 (d) National private industry best practices.

7 ~~(b) The office shall post the cybersecurity strategy on the~~
8 ~~Internet Web site of the office and transmit a copy to each~~
9 ~~secretary.~~

10 8592.45. (a) Each state agency shall report on ~~their~~ *its*
11 compliance with the standards developed pursuant to Section
12 8592.40 to the office in the manner and at the time directed by the
13 ~~office~~ *office*, but no later than January 1, 2019.

14 (b) ~~The office~~ *office, in conjunction with the Department of*
15 *Technology*, shall provide suggestions for a state agency to improve
16 compliance with the standards developed pursuant to Section
17 8592.40, if any, to the head of the state agency and the secretary
18 responsible for the state agency. For a state agency that is not under
19 the responsibility of a secretary, the office shall provide any
20 suggestions to the head of the state agency and the Governor.

21 8592.50 The report required by subdivision (a) of Section
22 8592.45 and any public records relating to any communication
23 made pursuant to, or in furtherance of the purposes of, subdivision
24 (b) of Section 8592.45 are confidential and shall not be disclosed
25 pursuant to any state law, including, but not limited to, the
26 California Public Records Act (Chapter 3.5 (commencing with
27 Section 6250) of Division 7 of Title 1).

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

36 Preventing public disclosure of the individual cybersecurity
37 preparations of state agencies promotes public safety by prohibiting

- 1 access to those who would use that information to thwart the
- 2 cybersecurity of critical infrastructure within the state.

O