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.

LEGISLATIVE COUNSEL'S DIGEST

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

(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.

This bill would require the Office of Emergency Services to ~~develop and~~ transmit to the ~~Legislature a state-wide emergency services response plan for cybersecurity attacks on critical infrastructure systems, as defined.~~ *Legislature, on or before July 1, 2017, the Cyber Security Annex to the State Emergency Plan, also known as Emergency Function 18 or EF 18.* The bill would further require the office to develop a comprehensive cybersecurity strategy setting standards for state agencies, as defined, ~~and private entities to~~ *to, among other things,* prepare for cybersecurity ~~attacks on~~ *interference with, or the compromise or incapacitation of,* critical infrastructure ~~systems. The bill~~ *and* would require state ~~agencies, and authorize private entities,~~ *agencies* to report its ~~cybersecurity strategy~~ *compliance with these standards* to the office. The bill would require the office to provide suggestions for ~~improvement to the cybersecurity strategy of a state agency, and authorize the office~~

~~to do the same for a private entity, but only for purposes of protecting public health and safety.~~ *a state agency to improve compliance with these standards.* The bill would prohibit public disclosure of ~~the office's state-wide emergency services response plan and~~ *public records relating to* the ~~individual~~ cybersecurity strategies of state ~~agencies and private entities.~~ *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 ~~and private~~ enterprises has resulted in an abundance of public access to information and services provided by the ~~government and businesses,~~ *government,* but the increased interdependence ~~on~~ *of* information technology systems has created a new type of risk for society. ~~Cybersecurity threats~~ *Threats* to public ~~and private~~ critical infrastructure ~~systems~~ that use information technology within the state present risks to public health and safety and could severely disrupt ~~private~~ economic activity within California.

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

(c) A comprehensive cybersecurity strategy, undertaken in a coordinated effort between ~~federal and state governments and private entities,~~ *state agencies,* will help prepare for ~~cyberattacks on these~~ *threats to* critical ~~infrastructure systems,~~ *infrastructure,* thereby reducing the potential consequences from those attacks.

(d) 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 ~~the proper~~ *a* state entity *appropriate* to develop, implement, and manage a comprehensive cybersecurity strategy, undertaken in a coordinated effort between ~~federal and state governments and private entities,~~ *state agencies,* to protect ~~these~~ critical ~~infrastructure systems from attacks to cybersecurity.~~ *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 ~~a cyberattack.~~ *an interference with, or the compromise or incapacitation of, critical infrastructure.*

(e) It is the intent of the Legislature in enacting this legislation to develop a comprehensive cybersecurity strategy, undertaken in a coordinated effort between ~~federal and state governments and private entities,~~ *state agencies,* to prepare California for ~~cyberattacks on~~ *threats to* critical infrastructure ~~systems~~ 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. (a) For purposes of this article, "critical infrastructure systems" shall mean a public or private information technology system that services any of the following sectors:~~

~~(1) Communications.~~

~~(2) Emergency services.~~

~~(3) Energy.~~

~~(4) Financial Services.~~

~~(5) Food and Agriculture.~~

~~(6) Healthcare and public health.~~

~~(7) Transportation systems.~~

~~(8) Water and wastewater systems.~~

~~(b)~~

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

(a) "Critical infrastructure" means systems and assets so vital to the state that the incapacity or destruction of those systems or assets would have a debilitating impact on security, economic

security, public health and safety, or any combination of those matters.

(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 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.

(2) The ability of critical infrastructure 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.

(3) Any planned or past operational problem or solution regarding critical infrastructure, 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.

(c) "Secretary" ~~shall mean~~ *means* the secretary of each state agency as set forth in subdivision (a) of Section 12800.

~~(c)~~

(d) "State agency" or "state agencies" ~~shall have~~ *means* the same ~~meaning~~ as "state agency" as set forth in Section 11000.

8592.35. (a) On or before July 1, 2017, the office shall transmit to the Legislature ~~a state-wide emergency services response plan for cybersecurity attacks on critical infrastructure systems~~ *the Cyber Security Annex to the State Emergency Plan, also known as 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 state-wide 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) ~~Notwithstanding Section 9795, the~~ *The* office shall transmit the plan to the Legislature ~~by providing a printed copy to the Secretary of the Senate and the Chief Clerk of the Assembly.~~ *pursuant to Section 9795.*

8592.40. (a) On or before July 1, 2018, the office shall develop a comprehensive cybersecurity strategy setting standards for state agencies ~~and private entities~~ to prepare for cybersecurity ~~attacks on~~ *interference with, or the compromise or incapacitation of,* critical infrastructure ~~systems.~~ *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:

(1) Costs to implement the standards.

~~(2) Regional business impacts.~~

~~(3) National~~

(2) Security of critical infrastructure information.

(3) Centralized management of risk.

(4) National private industry best practices.

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

8592.45. (a) Each state agency shall ~~transmit a cybersecurity strategy that meets the standards set forth in~~ *report on their compliance with the standards developed pursuant to* Section 8592.40 to the office in the manner and at the time directed by the ~~office.~~ *office but no later than January 1, 2019.*

(b) The office shall provide suggestions for ~~improvement to the cybersecurity strategy of a state agency, if any,~~ *a state agency to improve compliance with the standards developed pursuant to Section 8592.40, 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 shall provide *any* suggestions ~~for improvement to a cybersecurity strategy, if any,~~ to the head of the state agency and the Governor.

~~8592.50. (a) A private entity may transmit a cybersecurity strategy that meets the standards set forth in Section 8592.40 to the office.~~

~~(b) The office shall review and provide suggestions for improvement, if any, to the cybersecurity strategy of a private entity for the purposes of protecting public health and safety, and~~

~~shall not review or make suggestions to the cybersecurity strategy of a private entity solely for the private benefit of the private entity.~~

~~8592.55.~~

8592.50 ~~(a)~~ The ~~plan required by Section 8592.35, a state agency cybersecurity strategy~~ *report* required by *subdivision (a) of* Section ~~8592.45, or a private entity cybersecurity strategy authorized by Section 8592.50 are~~ *8592.45 and any public records relating to any communication made pursuant to, or in furtherance of the purposes of, subdivision (b) of Section 8592.45 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).

~~(b) The report to the Legislature required by Section 8592.35 shall not be subject to production pursuant to the Legislative Open Records Act (Article 3.5 (commencing with Section 9070) of Chapter 1.5 of Part 1 of Division 2).~~

SEC. 3. The Legislature finds and declares that Section 2 of this act, which adds Section ~~8592.55~~ *8592.50* 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 ~~Office of Emergency Services' state-wide emergency services response plan for cybersecurity attacks on critical infrastructure systems and the~~ individual cybersecurity ~~strategies~~ *preparations* of state agencies ~~and private entities~~ promotes public safety by prohibiting access to those who would use that information to thwart the cybersecurity of critical infrastructure ~~systems~~ within the state.

O