ASSEMBLY BILL No. 2200

Introduced by Assembly Member John A. Pérez

February 20, 2014

An act to add and repeal Chapter 4.5 (commencing with Section 8305) of Division 1 of Title 2 of the Government Code, relating to cyber security.

LEGISLATIVE COUNSEL'S DIGEST

AB 2200, as introduced, John A. Pérez. California Cyber Security Commission.

Existing law establishes various advisory boards and commissions in state government with specified duties and responsibilities.

This bill would create the California Cyber Security Commission consisting of members comprised of representatives from state, local, and federal government, the Legislature, and private industries, as specified. The duties of the commission would include establishing cyber-attack response strategies and defining a hierarchy of command within the state for this purpose. The bill would require the commission to meet on a monthly basis, and would require the commission to issue a report on a quarterly basis to the Governor's Office and the Legislature that details the cyber security status and progress of the state and makes recommendations on how to improve the cyber security of the state.

This bill would abolish the commission, and repeal these provisions, on January 1, 2020.

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. Chapter 4.5 (commencing with Section 8305) is added to Division 1 of Title 2 of the Government Code, to read:

Chapter 4.5. California Cyber Security Commission

8305. The Legislature finds and declares all of the following:

(a) The State of California's growing dependence on technology has made it increasingly vulnerable to both foreign and domestic cyber security attacks. Thus far, there has been a fragmented approach to this issue with independent efforts occurring through federal, state, and local government, as well as in the state's universities and within private industry. For the purposes of public safety and protection of public assets, the state has a role in coordinating and improving its overall security and response capabilities.

(b) The market for cyber security is estimated to be more than seventy billion dollars ($70,000,000,000) in 2014. Of that amount, sixty-seven billion dollars ($67,000,000,000) is estimated to be spent nationally by private companies for computer and network security and the United States Department of Defense is planning to spend four billion six hundred million dollars ($4,600,000,000). The United States Department of Defense is planning on spending twenty-three billion dollars ($23,000,000,000) over the next five years. Overall spending is expected to increase rapidly as recognition of threats becomes more ubiquitous. The California economy stands to greatly benefit from this industry growth.

(c) The State of California has already made investments for the purpose of cyber security; examples of which are research funding for the Lawrence Livermore National Laboratory and funding to augment a cyber security assessment and response team within the California National Guard.

(d) The California Cyber Security Task Force was initiated in May 2013 for the purposes of identifying critical threats, assembling primary stakeholders, and highlighting the growing importance of the issue. Among other things, this has increased awareness of the state's compliance with the new federal National Institute of Standards and Technology (NIST) standards and the

Office of Emergency Services establishing Emergency Function 18, created particularly for cyber security.

(e) Over 50,000 new malicious online activities are identified every day, according to the United States Department of Defense. Incidents of sophisticated and well-coordinated attacks and data breaches are occurring more regularly, the average cost of which amounts to more than ten million dollars ($10,000,000). In 2012, a data breach to the state of South Carolina required more than twenty million dollars ($20,000,000) in response and restitution. The State of California is vulnerable technically, legally, and financially to these threats.

8305.1. (a) There is in the state government the California Cyber Security Commission. The commission shall consist of the following members:

(1) The Director of Emergency Services and his or her designee with knowledge, expertise, and decisionmaking authority with respect to the Office of Emergency Services's information technology and information security. The director may designate an individual to serve on his or her behalf if the individual has knowledge, expertise, and decisionmaking authority with respect to the Office of Emergency Services's information technology and information security.

(2) The Adjutant General of the Military Department and his or her designee with knowledge, expertise, and decision making authority with respect to the Military Department's information technology and information security. The Adjutant General may designate an individual to serve on his or her behalf if the individual has knowledge, expertise, and decisionmaking authority with respect to the Military Department's information technology and information security.

(3) The Director of Technology, or his or her designee to serve on his or her behalf if the individual has knowledge, expertise, and decisionmaking authority with respect to the Department of Technology's information technology and information security.

(4) The Chief of the Office of Information Security, or his or her designee to serve on his or her behalf if the individual has knowledge, expertise, and decisionmaking authority with respect to the office's information technology and information security.

(5) The Commission President of the Public Utilities Commission, or his or her designee to serve on his or her behalf

if the individual has knowledge, expertise, and decisionmaking authority with respect to the commission's information technology and information security.

(6) The Director of Transportation, or his or her designee to serve on his or her behalf if the individual has knowledge, expertise, and decisionmaking authority with respect to the Department of Transportation's information technology and information security.

(7) The Insurance Commissioner, or his or her designee to serve on his or her behalf if the individual has knowledge, expertise, and decisionmaking authority with respect to the Department of Insurance's information technology and information security.

(8) The State Public Health Officer, or his or her designee to serve on his or her behalf if the individual has knowledge, expertise, and decisionmaking authority with respect to the State Department of Public Health's information technology and information security.

(9) Four representatives appointed by the Governor who meet the following requirements:

(A) A representative of the University of California who has done research in the area of information technology and information security.

(B) A representative of the California State University who has done research in the area of information technology and information security.

(C) A representative from a private university in California who has done research in the area of information technology and information security.

(D) A representative from the Lawrence Livermore National Laboratory or Lawrence Berkeley National Laboratory who has done research in the area of information technology and information security.

(10) Three representatives appointed by the Governor who meet the following requirements:

(A) A representative from the Bureau of Investigations or the Federal Bureau of Investigation who has knowledge, expertise, and experience with enforcement or prosecution of cyber crimes.

(B) A representative from the Department of the California Highway Patrol who has knowledge, expertise, and experience with enforcement or prosecution of cyber crimes.

(C) A representative from the Department of Justice who has knowledge, expertise, and experience with enforcement or prosecution of cyber crimes.

(11) Three representatives from local government who have knowledge, expertise, and experience with emergency response to information security breaches. One representative shall be appointed by the Governor, one representative shall be appointed by the Speaker of the Assembly, and one representative shall be appointed by the Senate Committee on Rules.

(12) Four representatives from the retail, finance, utilities, health care, or technology industries who have knowledge, expertise, and experience with information technology and information security. Two representatives shall be appointed by the Governor, one representative shall be appointed by the Speaker of the Assembly, and one representative shall be appointed by the Senate Committee on Rules.

(13) Two representatives who are chairpersons from committees of the Assembly that address information technology and information security, who shall be appointed by the Speaker of the Assembly. These representatives shall serve as nonvoting members in an advisory capacity.

(14) Two representatives who are chairpersons from committees of the Senate that address information technology and information security, who shall be appointed by the Senate Committee on Rules. These representatives shall serve as nonvoting members in an advisory capacity.

(b) The commission may also include two representatives from the United States Department of Homeland Security who have knowledge, expertise, and experience in the area of information technology and information security, who serve in a voluntary capacity and as nonvoting members.

(c) The Director of Emergency Services and the Director of Technology, or their designees to serve on their behalves if those individuals have knowledge, expertise, and experience with information technology and information security, shall serve as cochairs of the commission.

(d) Twenty members shall constitute a quorum for the transaction of business, and all official acts of the commission shall require the affirmative vote of a majority of its members constituting a quorum.

(e) The members of the commission shall serve without compensation, except that each member of the commission shall be entitled to receive his or her actual necessary traveling expenses while on official business of the commission.

8305.2. The commission shall meet monthly, commencing in January 2015.

8305.3. (a) The commission shall focus on improving the state's cyber security and cyber response capabilities by developing partnerships with the public and private sector as well as the academic and nongovernmental world to share cyber security and cyber threat information to enable state government to protect and secure important information and data, intellectual property, financial networks, and critical infrastructure.

(b) The duties of the commission shall include, but not be limited to, the following:

(1) Working with the United States Department of Homeland Security to define a system of information sharing regarding cyber threat monitoring and response.

(2) Recommending minimum security standards for all state agencies.

(3) Researching in conjunction with academia and others to expand and improve state cyber security capability.

(4) Expanding public-private cyber security partnerships.

(5) Establishing cyber-attack response strategies and defining a hierarchy of command within the state for this purpose.

(6) Providing training for state employees and others to produce credentialed cyber security employees.

(7) Developing with the Department of Insurance a strategy to acquire cyber insurance for state agencies and assets.

(8) Proposing potential governmental reorganization to enhance the state's cyber security and response capabilities.

(9) Exploring fiscal options to fund the commission and its various activities, including the activities of some of its specific members, including the California National Guard's computer network defense team (CND).

(c) The commission shall issue a report on a quarterly basis to the Governor's Office and the Legislature that details the cyber security status and progress of the state and makes recommendations on how to improve the cyber security of the

state. The reports shall be submitted in compliance with Section 9795.

8305.4. This chapter shall become inoperative on January 1, 2020, and shall be repealed as of that date.

O