ASSEMBLY BILL No. 1172

Introduced by Assembly Member Chau

February 27, 2015

An act to add and repeal Article 3.9 (commencing with Section 8574.50) of Chapter 7 of Division 1 of Title 2 of the Government Code, relating to cyber security.

LEGISLATIVE COUNSEL'S DIGEST

AB 1172, as introduced, Chau. California cyber security.

Existing law establishes various advisory boards and commissions in state government with specified duties and responsibilities. Existing law establishes in state government the Governor's Office of Emergency Services and the Department of Technology.

This bill would continue in existence the California Cyber Security Task Force, consisting of specified members, previously created by the Governor's Office of Emergency Services and the Department of Technology, in the Governor's Office of Emergency Services. This bill would authorize the task force to convene stakeholders to act in an advisory capacity and compile policy recommendations on cyber security for the state. The bill would require the task force to meet quarterly, or more often as necessitated by emergency circumstances. This bill would require the task force to complete and issue a report of policy recommendations to the Governor's office and the Legislature. This bill would also require the task force to perform specified functions relating to cyber security. This bill would create a State Director of Cyber Security with specified duties within the Governor's Office of Emergency Services. This bill would 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. Article 3.9 (commencing with Section 8574.50) is added to Chapter 7 of Division 1 of Title 2 of the Government Code, to read:

Article 3.9. California Cyber Security

8574.50. (a) There is hereby continued in existence the California Cyber Security Task Force, created in 2013 by the Governor's Office of Emergency Services and the Department of Technology, in the Governor's Office of Emergency Services.

(b) The California Cyber Security Task Force shall consist of the following members:

(1) The Director of Emergency Services, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the Office of Emergency Services' information technology and information security duties.

(2) The Director of the Department of Technology, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the director's information technology and information security duties set forth in Chapter 5.6 (commencing with Section 11545).

(3) The Attorney General, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the Department of Justice's information technology and information security.

(4) The Adjutant General of the Military Department, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the Military Department's information technology and information security.

(5) The Commissioner of the California Highway Patrol, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the Department of the California Highway Patrol's information technology and information security.

(6) A representative of the Public Utilities Commission or California Energy Commission with knowledge, expertise, and

decisionmaking authority with respect to information technology and information security, who shall be appointed by the Governor.

(7) An individual with cyber security expertise, who shall be appointed by the Governor.

(8) An individual with cyber security expertise, who shall be appointed by the Senate Committee on Rules.

(9) An individual with cyber security expertise, who shall be appointed by the Speaker of the Assembly.

(c) The California Cyber Security Task Force may convene stakeholders, both public and private, to act in an advisory capacity and compile policy recommendations on cyber security for the state of California. The California Cyber Security Task Force shall complete and issue a report of policy recommendations to the Governor's office and the Legislature on an annual basis. The report shall be completed in compliance with Section 9795.

(d) The California Cyber Security Task Force shall meet quarterly, or more often as necessitated by emergency circumstances, within existing resources to ensure that the policy recommendations from the report are implemented and any necessary modifications that may arise are addressed in a timely manner.

(e) The Governor's Office of Emergency Services and the Department of Technology may conduct the strategic direction of risk assessments performed by the Military Department's Computer Network Defense Team as budgeted in Item 8940-001-0001 of the Budget Act of 2014.

8574.51. There is within the Governor's Office of Emergency Services a State Director of Cyber Security, who shall do all of the following:

(a) Be the Executive Director of the California Cyber Security Task Force.

(b) Provide strategic direction of risk assessments performed with state resources.

(c) Complete a risk profile of state assets and capabilities for the purpose of compiling statewide contingency plans including, but not limited to, Emergency Function 18 of the State Emergency Plan.

(d) Act as point of contact to the federal government and private entities within the state in the event of a relevant emergency as declared by the Governor.

(e) Be the Governor's Office of Emergency Services and the Department of Technology on cyber security.

8574.52. The Cyber Security Task Force shall perform the following functions based on the following priorities:

(a) Develop within state government cyber prevention, defense, and response strategies and defining a hierarchy of command within the state for this purpose. This duty includes, but is not limited to, the following activities:

(1) Ensuring the continual performance of risk assessments on state information technology systems. The assessments shall include penetration tests, vulnerability scans, and other industry-standard methods that identify potential risk.

(2) Using assessment results and other state-level data to create a risk profile of public assets, critical infrastructure, public networks, and private operations susceptible to cyber-attacks. The risk profile shall include the development of statewide contingency plans including, but not limited to, Emergency Function 18 of the State Emergency Plan.

(b) Partner with the United States Department of Homeland Security to develop an appropriate information sharing system that allows for a controlled and secure process to effectively disseminate cyber threat and response information and data to relevant private and public sector entities. This information sharing system shall reflect state priorities and target identified threat and capability gaps.

(c) Provide recommendations for information technology security standards for all state agencies using, among other things, protocols established by the National Institute for Standards and Technology and reflective of appropriate state priorities.

(d) Compile and integrate, as appropriate, the research conducted by academic institutions, federal laboratories, and other cyber security experts into state operations and functions.

(e) Expand the state's public-private cyber security partnership network.

(f) Expand collaboration with the state's law enforcement apparatus assigned jurisdiction to prevent, deter, investigate, and prosecute cyber attacks and information technology crime, including collaboration with entities like the High-Tech Theft Apprehension Program, and its five regional task forces, the Department of the California Highway Patrol, and the Attorney

General's eCrimes unit. Collaboration shall include information sharing that will enhance their capabilities including assistance to better align their activities with federal and local resources, provide additional resources, and extend their efforts into regions of the state not currently represented.

(g) Propose, where appropriate, potential operational or functional enhancement to the state's cyber security assessment and response capabilities, as well as investment or spending recommendation and guidance for the state's information technology budget and procurement.

8574.53. The California Cyber Security Task Force shall take all necessary steps to protect personal information and privacy, public and private sector data, and the constitutional rights and liberties of individuals, when implementing its duties.

8574.54. (a) The California Cyber Security Task Force may issue reports, in addition to the report described in subdivision (c) of Section 8574.51, to the Governor's office and the Legislature detailing the activities of the task force, including, but not limited to, progress on the California Cyber Security Task Force's various tasks and actions taken and recommended in response to an incident, as appropriate.

(b) The reports shall be submitted in compliance with Section 9795.

8574.55. The California Cyber Security Task Force may engage or accept the services of agency or department personnel, accept the services of stakeholder organizations, and accept federal, private, or other nonstate funding, to operate, manage, or conduct the business of the California Cyber Security Task Force.

8574.56. Each department and agency shall cooperate with the California Cyber Security Task Force and furnish it with information and assistance that is necessary or useful to further the purposes of this article.

8574.57. This article shall become inoperative on January 1, 2020, and shall be repealed as of that date.

O