

AMENDED IN SENATE JULY 2, 2015

CALIFORNIA LEGISLATURE—2015–16 REGULAR SESSION

ASSEMBLY BILL

No. 1172

Introduced by Assembly Member Chau
(Coauthor: Assembly Member Cooper)

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 amended, 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:

1 SECTION 1. Article 3.9 (commencing with Section 8574.50)
2 is added to Chapter 7 of Division 1 of Title 2 of the Government
3 Code, to read:

4
5 Article 3.9. California Cyber Security
6

7 8574.50. (a) There is hereby continued in existence the
8 California Cyber Security Task Force, created in 2013 by the
9 Governor’s Office of Emergency Services and the Department of
10 Technology, in the Governor’s Office of Emergency Services.

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

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

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

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

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

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

1 (6) A representative of the Public Utilities Commission or
2 California Energy Commission with knowledge, expertise, and
3 decisionmaking authority with respect to information technology
4 and information security, who shall be appointed by the Governor.

5 (7) ~~An individual with cyber security expertise,~~ *A representative*
6 *from the utility or energy industry,* who shall be appointed by the
7 Governor.

8 (8) ~~An individual with cyber security expertise,~~ *A representative*
9 *from law enforcement,* who shall be appointed by the ~~Senate~~
10 ~~Committee on Rules.~~ *Governor.*

11 (9) ~~An individual~~ *Three individuals* with cyber security
12 expertise, who shall be ~~appointed~~ *appointed, one each,* by the
13 *Governor, the Senate Rules Committee, and the Speaker of the*
14 *Assembly.*

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

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

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

33 8574.51. There is within the Governor’s Office of Emergency
34 Services a State Director of Cyber Security, *appointed by the*
35 *Governor and confirmed by the Senate,* who shall do all of the
36 following:

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

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

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

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

8 (e) Be *an adviser to* the Governor's Office of Emergency
9 Services and the Department of Technology on cyber security.

10 8574.52. The Cyber Security Task Force shall perform the
11 following functions based on the following priorities:

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

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

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

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

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

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

1 (e) Expand the state’s public-private cyber security partnership
2 network.

3 (f) Expand collaboration with the state’s law enforcement
4 apparatus assigned jurisdiction to prevent, deter, investigate, and
5 prosecute cyber attacks and information technology crime,
6 including collaboration with entities like the High-Tech Theft
7 Apprehension Program, and its five regional task forces, the
8 Department of the California Highway Patrol, and the Attorney
9 General’s eCrimes unit. Collaboration shall include information
10 sharing that will enhance their capabilities including assistance to
11 better align their activities with federal and local resources, provide
12 additional resources, and extend their efforts into regions of the
13 state not currently represented.

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

19 8574.53. The California Cyber Security Task Force shall take
20 all necessary steps to protect personal information and privacy,
21 public and private sector data, and the constitutional rights and
22 liberties of individuals, when implementing its duties.

23 8574.54. (a) The California Cyber Security Task Force may
24 issue reports, in addition to the report described in subdivision (c)
25 of Section 8574.51, to the Governor’s office and the Legislature
26 detailing the activities of the task force, including, but not limited
27 to, progress on the California Cyber Security Task Force’s various
28 tasks and actions taken and recommended in response to an
29 incident, as appropriate.

30 (b) The reports shall be submitted in compliance with Section
31 9795.

32 8574.55. The California Cyber Security Task Force may engage
33 or accept the services of agency or department personnel, accept
34 the services of stakeholder organizations, and accept federal,
35 private, or other nonstate funding, to operate, manage, or conduct
36 the business of the California Cyber Security Task Force.

37 8574.56. Each department and agency shall cooperate with the
38 California Cyber Security Task Force and furnish it with
39 information and assistance that is necessary or useful to further
40 the purposes of this article.

1 8574.57. This article shall become inoperative on January 1,
2 2020, and shall be repealed as of that date.

O