GOVERNMENT CODE - GOV

TITLE 2. GOVERNMENT OF THE STATE OF CALIFORNIA [8000 - 22980] *(Title 2 enacted by Stats. 1943, Ch. 134.)*

DIVISION 1. GENERAL [8000 - 8899.95] *(Division 1 enacted by Stats. 1943, Ch. 134.)*

CHAPTER 7. California Emergency Services Act [8550 - 8669.87] *(Chapter 7 added by Stats. 1970, Ch. 1454.)*

ARTICLE 6.4. Cybersecurity [8592.30 - 8592.50] *(Article 6.4 added by Stats. 2016, Ch. 508, Sec. 2.)*

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

(a) “Critical infrastructure controls” means networks and systems controlling assets so vital to the state that the incapacity or destruction of those networks, systems, or assets would have a debilitating impact on public health, safety, economic security, or any combination thereof.

(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 controls 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 or harms public health, safety, or economic security, or any combination thereof.

(2) The ability of critical infrastructure controls 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.

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

(c) “Department” means the Department of Technology.

(d) “Office” means the Office of Emergency Services.

(e) “Secretary” means the secretary of each state agency as set forth in subdivision (a) of Section 12800.

(f) “State agency” or “state agencies” means the same as “state agency” as set forth in Section 11000.

(Added by Stats. 2016, Ch. 508, Sec. 2. (AB 1841) Effective January 1, 2017.)

8592.35. (a) (1) On or before July 1, 2018, the department shall, in consultation with the office and compliance with Section 11549.3, update the Technology Recovery Plan element of the State Administrative Manual to ensure the inclusion of cybersecurity strategy incident response standards for each state agency to secure its critical infrastructure controls and critical infrastructure information.

(2) In updating the standards in paragraph (1), the department shall consider, but not be limited to considering, all of the following:

(A) Costs to implement the standards.

(B) Security of critical infrastructure information.

(C) Centralized management of risk.

(D) Industry best practices.

(E) Continuity of operations.

(F) Protection of personal information.

(b) Each state agency shall provide the department with a copy of its updated Technology Recovery Plan.

(c) Each state agency shall, as part of its Technology Recovery Plan, provide the department with an inventory of all critical infrastructure controls, and their associated assets, in the possession of the agency.

(Amended by Stats. 2017, Ch. 790, Sec. 1. (AB 1022) Effective January 1, 2018.)

8592.40. (a) Each state agency shall report on its compliance with the standards updated pursuant to Section 8592.35 to the department in the manner and at the time directed by the department, but no later than July 1, 2019.

(b) At the request of the department, any local entity that receives state funds for the purposes of storing, sharing, or transmitting data, or in support of an information technology project with a state entity, may submit a Technology Recovery Plan, as specified by Section 8592.35, to the department.

(c) The department, in conjunction with the office, may provide suggestions for a state agency or local entity that provided a Technology Recovery Plan pursuant to subdivision (b) to improve compliance with the standards developed pursuant to Section 8592.35, if any, to the head of the state agency and the secretary responsible for the state agency or the head of the local entity. For a state agency that is not under the responsibility of a secretary, the department shall provide any suggestions to the head of the state agency and the Governor.

(Amended by Stats. 2017, Ch. 790, Sec. 2. (AB 1022) Effective January 1, 2018.)

8592.45. The information required by subdivisions (b) and (c) of Section 8592.35, the report required by subdivision (a) of Section 8592.40, the plan authorized by subdivision (b) of Section 8592.40, and any public records relating to any communication made pursuant to, or in furtherance of the purposes of, subdivision (c) of Section 8592.40 are confidential and shall not be disclosed pursuant to any state law, including, but not limited to, the California Public Records Act (Division 10 (commencing with Section 7920.000) of Title 1).

(Amended by Stats. 2021, Ch. 615, Sec. 155. (AB 474) Effective January 1, 2022. Operative January 1, 2023, pursuant to Sec. 463 of Stats. 2021, Ch. 615.)

8592.50. (a) (1) The office shall direct the California Cybersecurity Integration Center to prepare a strategic, multiyear outreach plan that focuses on ways to assist the food and agriculture sector and the water and wastewater sector in their efforts to improve cybersecurity and that includes, but is not limited to, all of the following:

(A) A description of the need for greater cybersecurity outreach and assistance to the food and agriculture sector and the water and wastewater sector.

(B) The goal of the outreach plan.

(C) Methods for coordinating with other state and federal agencies, nonprofit organizations, and associations that provide cybersecurity services or resources for the food and agricultural sector and the water and wastewater sector.

(D) An estimate of the funding needed to execute the outreach plan.

(E) Potential funding sources for the funding needed by the California Cybersecurity Integration Center for the plan.

(F) A plan to evaluate the success of the outreach plan that includes quantifiable measures of success.

(2) The office shall submit the outreach plan prepared pursuant to this subdivision to the Legislature, pursuant to Section 9795, no later than January 1, 2024. The requirement for submitting a report imposed by this paragraph is inoperative on January 1, 2028, pursuant to Section 10231.5.

(b) (1) The office shall direct the California Cybersecurity Integration Center to evaluate options for providing entities in the food and agriculture sector or the water and wastewater sector with grants or alternative forms of funding to improve cybersecurity preparedness. Upon completion of the evaluation, the office shall submit a report to the Legislature, pursuant to Section 9795, no later than January 1, 2024, that includes, but is not limited to, all of the following:

(A) A summary of the evaluation performed by the California Cybersecurity Integration Center.

(B) The specific grants and forms of funding for improved cybersecurity preparedness, including, but not limited to, the following:

(i) Current overall funding level.

(ii) Potential funding sources.

(C) Potential voluntary actions that do not require funding and assist the food and agriculture sector and the water and wastewater sector in their efforts to improve cybersecurity preparedness.

(2) The requirement for submitting a report imposed by this subdivision is inoperative on January 1, 2028, pursuant to Section 10231.5.

(Added by Stats. 2022, Ch. 820, Sec. 2. (SB 892) Effective January 1, 2023.)