Cal Gov Code § 11549.3

Deering's California Codes are current through the 2024 Regular Session Ch 1

Deering's California Codes Annotated > GOVERNMENT CODE (§§ 1 — 500000–500049) > Title 2 Government of the State of California (Divs. 1 — 5) > Division 3 Executive Department (Pts. 1 — 14) > Part 1 State Departments and Agencies (Chs. 1 — 11) > Chapter 5.7 Office of Information Security and Office of Privacy Protection (Arts. 1 — 2) > Article 1 Office of Information Security (§§ 11549 — 11549.4)

§ 11549.3. Information security program established; Responsibilities of program; Compliance with security and privacy policies, standards, and procedures; Independent security assessment

(a) The chief shall establish an information security program. The program responsibilities include, but are not limited to, all of the following:

(1) The creation, updating, and publishing of information security and privacy policies, standards, and procedures for state agencies in the State Administrative Manual.

(2) The creation, issuance, and maintenance of policies, standards, and procedures directing state agencies to effectively manage security and risk for both of the following:

(A) Information technology, which includes, but is not limited to, all electronic technology systems and services, automated information handling, system design and analysis, conversion of data, computer programming, information storage and retrieval, telecommunications, requisite system controls, simulation, electronic commerce, and all related interactions between people and machines.

(B) Information that is identified as mission critical, confidential, sensitive, or personal, as defined and published by the office.

(3) The creation, issuance, and maintenance of policies, standards, and procedures directing state agencies for the collection, tracking, and reporting of information regarding security and privacy incidents.

(4) The creation, issuance, and maintenance of policies, standards, and procedures directing state agencies in the development, maintenance, testing, and filing of each state agency's disaster recovery plan.

(5) Coordination of the activities of state agency information security officers, for purposes of integrating statewide security initiatives and ensuring compliance with information security and privacy policies and standards.

(6) Promotion and enhancement of the state agencies' risk management and privacy programs through education, awareness, collaboration, and consultation.

(7) Representing the state before the federal government, other state agencies, local government entities, and private industry on issues that have statewide impact on information security and privacy.

(b) All state entities defined in Section 11546.1 shall implement the policies and procedures issued by the office, including, but not limited to, performing both of the following duties:

(1) Comply with the information security and privacy policies, standards, and procedures issued pursuant to this chapter by the office.

(2) Comply with filing requirements and incident notification by providing timely information and reports as required by the office.

(c)

(1) The office may conduct, or require to be conducted, an independent security assessment of every state agency, department, or office. The cost of the independent security assessment shall be funded by the state agency, department, or office being assessed.

(2) In addition to the independent security assessments authorized by paragraph (1), the office, in consultation with the Office of Emergency Services, shall perform all the following duties:

(A) Annually require no fewer than 35 state entities to perform an independent security assessment, the cost of which shall be funded by the state agency, department, or office being assessed.

(B) Determine criteria and rank state entities based on an information security risk index that may include, but not be limited to, analysis of the relative amount of the following factors within state agencies:

(i) Personally identifiable information protected by law.

(ii) Health information protected by law.

(iii) Confidential financial data.

(iv) Self-certification of compliance and indicators of unreported noncompliance with security provisions in the following areas:

(I) Information asset management.

(II) Risk management.

(III) Information security program management.

(IV) Information security incident management.

(V) Technology recovery planning.

(C) Determine the basic standards of services to be performed as part of independent security assessments required by this subdivision.

(3) The Military Department may perform an independent security assessment of any state agency, department, or office, the cost of which shall be funded by the state agency, department, or office being assessed.

(d) State agencies and entities required to conduct or receive an independent security assessment pursuant to subdivision (c) shall transmit the complete results of that assessment and recommendations for mitigating system vulnerabilities, if any, to the office and the Office of Emergency Services.

(e) The office shall report to the Department of Technology and the Office of Emergency Services any state entity found to be noncompliant with information security program requirements.

(f)

(1) Every state agency, as defined in Section 11000, that is not subject to subdivision (b) shall do all of the following:

(A) Adopt and implement information security and privacy policies, standards, and procedures that adhere to the following standards:

(i) The National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, and its successor publications.

(ii) Federal Information Processing Standards (FIPS) 199 Standards for Security Categorization of Federal Information and Information Systems, and its successor publications.

(iii) Federal Information Processing Standards (FIPS) 200 Minimum Security Requirements for Federal Information and Information Systems, and its successor publications.

(B) Perform a comprehensive, independent security assessment every two years. The independent assessment shall assess all policies, standards, and procedures adopted pursuant to subparagraph (A) and paragraph (2), if applicable.

(2) A state agency described in paragraph (1) may adopt and implement information security and privacy policies, standards, and procedures following Chapter 5300 - Information Technology - Office of Information Security of the State Administrative Manual. A state agency described in paragraph (1) may discontinue a policy, standard, or procedure adopted pursuant to this paragraph at any time.

(3) A state agency described in paragraph (1) may contract with the Military Department, or with a qualified responsible vendor, to perform an independent security assessment of the state agency pursuant to subparagraph (B) of paragraph (1), the cost of which shall be funded by the state agency being assessed.

(4)

(A) Every state agency described in paragraph (1) shall certify, on a form developed pursuant to subparagraph (C), by February 1 annually, to the office that the agency is in compliance with all policies, standards, and procedures adopted pursuant to this subdivision. The certification shall include a plan of action and milestones.

(B) Notwithstanding any other law, the certification made to the office shall be kept confidential and shall not be disclosed, except as provided in subparagraph (E). The office shall ensure the transferring, receiving, possessing, or disclosing of certifications is done in a manner that ensures the confidentiality and security of the certification, including restricting transfer and storage methods to electronic means and ensuring that certification data is encrypted in transport and at rest. The office shall only provide access to certifications to employees who have submitted to a criminal background check as a condition of employment.

(C) The office shall develop a form for certification based on the Statewide Information Management Manual (SIMM) 5330-B, making modifications as necessary to encompass the requirements on state agencies under paragraphs (1) to (4), inclusive.

(D) The office may make recommendations and offer assistance to any state agency described in paragraph (1) on completing the plan of action and milestones required under

paragraph (A). However, the office shall not have the authority to require any recommendation be followed or to compel acceptance of any assistance.

(E) The office shall review the certifications and make an annual summary report available, by May 1, 2024, and by March 1 every year thereafter, to the appropriate legislative committees and the Legislative Analyst's Office to further their oversight and budgetary responsibilities.

(5) As an alternative to complying with the requirements of paragraphs (1) to (4), inclusive, a state agency described in paragraph (1) may annually submit, by January 15, a declaration to the chief confirming that the state agency voluntarily and fully complies with subdivisions (b) and (c).

(6) This subdivision shall apply to the University of California only to the extent that the Regents of the University of California, by resolution, make any of these provisions applicable to the University.

(g)

(1) Notwithstanding any other law, during the process of conducting an independent security assessment pursuant to subdivision (c) or (f), information and records concerning the independent security assessment are confidential and shall not be disclosed, except that the information and records may be transmitted to state employees and state contractors who have been approved as necessary to receive the information and records to perform that independent security assessment, subsequent remediation activity, or monitoring of remediation activity.

(2) The results of a completed independent security assessment performed pursuant to subdivision (c), (f), or (j), and any related information shall be subject to all disclosure and confidentiality provisions 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), but not limited to Section 7929.210.

(h) The office may conduct or require to be conducted an audit of information security to ensure program compliance.

(i) The office shall notify the Office of Emergency Services, Department of the California Highway Patrol, and the Department of Justice regarding any criminal or alleged criminal cyber activity affecting any state entity or critical infrastructure of state government.

(j)

(1) At the request of a local educational agency, and in consultation with the California Cybersecurity Integration Center, the Military Department may perform an independent security assessment of the local educational agency, or an individual schoolsite under its jurisdiction, the cost of which shall be funded by the local educational agency.

(2) The criteria for the independent security assessment shall be established by the Military Department in coordination with the local educational agency.

(3) The Military Department shall disclose the results of an independent security assessment only to the local educational agency and the California Cybersecurity Integration Center.

(4) For purposes of this subdivision, "local educational agency" means a school district, county office of education, charter school, or state special school.

History

Added Stats 2007 ch 183 § 7 (SB 90), effective January 1, 2008. See this section as modified in Governor's Reorganization Plan No. 1 § 24 of 2009. Amended Stats 2010 ch 404 § 29 (AB 2408), effective January 1, 2011. See this section as modified in Governor's Reorganization Plan No. 2 § 195 of 2012; Amended Stats 2013 ch 356 § 6 (SB 96), effective September 26, 2013; Stats 2015 ch 518 § 1 (AB 670), effective January 1, 2016; Stats 2021 ch 77 § 11 (AB 137), effective July 16, 2021; Stats 2021 ch 615 § 166 (AB 474), effective January 1, 2022 (ch 593 prevails); Stats 2021 ch 593 § 1 (AB 1352), effective January 1, 2022; Stats 2022 ch 773 § 2 (AB 2135), effective January 1, 2023; Stats 2023 ch 45 § 15 (AB 127), effective July 10, 2023.

End of Document