AB-2135 Information security. (2021-2022)

Date Published: 10/03/2022 02:00 PM

Assembly Bill No. 2135

CHAPTER 773

An act to amend Section 11549.3 of the Government Code, relating to state government.

[Approved by Governor September 29, 2022. Filed with Secretary of State September 29, 2022.]

LEGISLATIVE COUNSEL'S DIGEST

AB 2135, Irwin. Information security.

Existing law establishes the Office of Information Security within the Department of Technology for the purpose of ensuring the confidentiality, integrity, and availability of state systems and applications and to promote and protect privacy as part of the development and operations of state systems and applications to ensure the trust of the residents of this state. The law requires an entity within the executive branch that is under the direct authority of the Governor to implement the policies and procedures issued by the office. The law additionally authorizes the office to conduct, or require to be conducted, an independent security assessment of every state agency, department, or office, as specified. The law authorizes the Military Department to perform an independent security assessment of any state agency, department, or office.

This bill would require state agencies not covered by the provisions described above to adopt and implement information security and privacy policies, standards, and procedures based upon standards issued by the National Institute of Standards and Technology and the Federal Information Processing Standards, as specified. The bill would require these state agencies to perform a comprehensive, independent security assessment every 2 years and would authorize them to contract with the Military Department, or with a qualified responsible vendor, for that purpose.

This bill would require these state agencies to certify, by February 1 annually, to the President pro Tempore of the Senate and the Speaker of the Assembly that the agency is in compliance with all adopted policies, standards, and procedures and to include a plan of action and milestones, as specified. The bill would require that the certification be kept confidential and not be disclosed, except that the information and records would be allowed to be shared, maintaining a chain of custody, with the members of the Legislature and legislative employees, at the discretion of the President pro Tempore of the Senate or the Speaker of the Assembly.

Because the required certification would be made under penalty of perjury, the bill would expand the crime of perjury and would thereby impose a state-mandated local program.

Existing constitutional provisions require that a statute that limits the right of access to the meetings of public bodies or the writings of public officials and agencies be adopted with findings demonstrating the interest protected by the limitation and the need for protecting that interest.

This bill would make legislative findings to that effect.

The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.

This bill would provide that no reimbursement is required by this act for a specified reason.
Vote: majority Appropriation: no Fiscal Committee: yes Local Program: yes

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

SECTION 1. It is the intent of the Legislature to enact legislation based upon the recommendations of the California State Auditor contained in Report 2018-611 “Gaps in Oversight Contribute to Weakness in the State’s Information Security” released in July 2019.

SEC. 2. Section 11549.3 of the Government Code is amended to read:

11549.3. (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, by February 1 annually, to legislative leadership, consisting of the President pro Tempore of the Senate and the Speaker of the Assembly, 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, as described in either the March 2019 publication of the Statewide Information Management Manual (SIMM) Section 5305-C, or in the most recent publication of that section.

(B) Notwithstanding any other law, the certification made to legislative leadership shall be kept confidential and shall not be disclosed, except that the information and records may be shared, maintaining a chain of custody, with the members of the Legislature and legislative employees, at the discretion of either the President pro tempore of the Senate or the Speaker of the Assembly. Legislative leadership, or their designee, shall consult with the state agencies described in paragraph (1) on the policies and procedures for transferring, receiving, possessing, or disclosing certifications that ensure confidentiality and security of the certification. Legislative leadership, or their designee, shall consult with the state agencies described in paragraph (1) to determine the form required for the certification.

(5) 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.

SEC. 3. The Legislature finds and declares that Section 2 of this act, which amends Section 11549.3 of the Government Code, imposes a limitation on the public’s right of access to the meetings of public bodies or the writings of public officials and agencies within the meaning of Section 3 of Article I of the California Constitution. Pursuant to that constitutional provision, the Legislature makes the following findings to demonstrate the interest protected by this limitation and the need for protecting that interest:

The state has a very strong interest in protecting its information technology systems from intrusion because those systems contain confidential information and play a critical role in the performance of the duties of state government. Thus, information regarding the specific vulnerabilities of those systems must be protected to preclude use of that information to facilitate attacks on those systems.

SEC. 4. No reimbursement is required by this act pursuant to Section 6 of Article XIII B of the California Constitution because the only costs that may be incurred by a local agency or school district will be incurred because this act creates a new crime or infraction, eliminates a crime or infraction, or changes the penalty for a crime or infraction, within the meaning of Section 17556 of the Government Code, or changes the definition of a crime within the meaning of Section 6 of Article XIII B of the California Constitution.