

AMENDED IN ASSEMBLY APRIL 6, 2015

CALIFORNIA LEGISLATURE—2015–16 REGULAR SESSION

ASSEMBLY BILL

No. 670

Introduced by Assembly Member Irwin

February 25, 2015

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

LEGISLATIVE COUNSEL'S DIGEST

AB 670, as amended, Irwin. Security assessments.

Existing law establishes the Department of Technology within the Government Operations Agency, headed by the Director of Technology who is also known as the State Chief Information Officer. The department is responsible for the approval and oversight of information technology projects by, among other things, consulting with agencies during initial project planning to ensure that project proposals are based on well-defined programmatic needs.

Existing law establishes the Office of Technology Services within the department, under the supervision of the Chief of the Office of Technology Services, and sets forth its duties, including, but not limited to, the authority to conduct or require a security ~~assessments~~ *assessment* of any state agency, as prescribed.

This bill would, instead, require the office to conduct, or require, an assessment of every state agency at least once every 2 years and would require the state agency being audited to pay the costs of the security assessment. The bill would authorize the department to require agencies that are not in compliance to redirect available funding to pay the costs of the assessments. The bill would require the department to adopt standards, to be included within the State Administrative Manual, setting

forth the manner for the assessed agency to communicate the assessment results to the department.

This bill would authorize ~~the department and~~ the Governor’s Office of Emergency Services to jointly conduct the strategic direction of risk security assessments performed by the Military Department’s Computer Network Defense Team, and would require those assessments to contain certain elements.

Existing law requires that a statute that limits the public’s right of access to the meetings of public bodies or the writings of public officials and agencies be adopted with findings to demonstrate the interest protected by the limitation and the need for protecting that interest.

This bill would limit access to security assessment results, and would make findings to demonstrate the interest protected by the limitation and the need for protecting that interest.

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

3 11549.3. (a) The director shall establish an information security
4 program. The program responsibilities include, but are not limited
5 to, all of the following:

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

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

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

19 (B) Information that is identified as mission critical, confidential,
20 sensitive, or personal, as defined and published by the Office of
21 Information Security.

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

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

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

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

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

20 (b) An information security officer appointed pursuant to Section
21 11546.1 shall implement the policies and procedures issued by the
22 Office of Information Security, including, but not limited to,
23 performing both of the following duties:

24 (1) Comply with the information security and privacy policies,
25 standards, and procedures issued pursuant to this chapter by the
26 Office of Information Security.

27 (2) Comply with filing requirements and incident notification
28 by providing timely information and reports as required by policy
29 or directives of the office.

30 (c) The office shall conduct, or require to be conducted, an
31 independent security assessment of every state agency, department,
32 or office at least once every two years. The cost of the security
33 assessment shall be funded by the state agency, department, or
34 office being assessed. *The assessment results shall be made*
35 *available only to the assessed entity.* The assessment shall include,
36 ~~at a minimum,~~ *to the extent practicable,* all of the following
37 components, which shall be conducted in compliance with the
38 National Institute of Standards and Technology (NIST) Special
39 Publication (SP) 800-53 Controls:

40 (1) ~~A legal, policy, standards, and procedure compliance review.~~

- 1 ~~(2)~~
- 2 (1) Vulnerability ~~scanning~~; scanning, that includes, but is not
- 3 limited to, all of the following:
- 4 (A) Validation that IT systems have currently supported
- 5 software, with all necessary security patches and updates applied.
- 6 (B) Validation that system security configurations are in
- 7 compliance with NIST standards.
- 8 (C) Validation that the network architecture is arranged so as
- 9 to separate internal, publicly accessible, and external zones, along
- 10 with a mechanism to identify and alert on attempted intrusions.
- 11 ~~(3)~~
- 12 (2) Penetration ~~testing~~; testing, when determined appropriate
- 13 by the Governor’s Offices of Emergency Services.
- 14 (3) A report on the number, severity, and nature of identified
- 15 vulnerabilities and recommendations for remediation and risk
- 16 mitigation.
- 17 (d) The office shall report to the Department of Technology any
- 18 state agency found to be noncompliant with information security
- 19 program requirements.
- 20 (e) The Department of Technology may require that any agency
- 21 in noncompliance with subdivision (c) redirect any funds within
- 22 the agency’s budget, that may be legally expended for these
- 23 purposes, for the purposes of paying the costs of compliance with
- 24 subdivision (c).
- 25 (f) ~~The Department of Technology and the Governor’s Office~~
- 26 of Emergency Services may ~~jointly~~ conduct the strategic direction
- 27 of ~~risk security~~ assessments performed by the Military
- 28 Department’s Computer Network Defense Team, as budgeted in
- 29 Item 8940-001-0001 of the Budget Act of 2014. *Each assessment*
- 30 *shall include all of the following:*
- 31 (1) Contracting and negotiations with state agencies,
- 32 departments, and offices, or private entities to be assessed.
- 33 (2) Setting an assessment calendar to be followed by the CND-T.
- 34 (3) Prioritizing of incident response.
- 35 (g) The Department of Technology shall adopt standards, to be
- 36 included within the State Administrative Manual, setting forth the
- 37 manner for the assessed agency to communicate the assessment
- 38 results to the department, including, but not limited to, all of the
- 39 following:
- 40 ~~(1) Identification of vulnerabilities.~~

1 (1) Aggregated, statistical information relevant to the assessment
2 results, including, but not limited to, the number of identified
3 vulnerabilities categorized by high, medium, and low risk. These
4 results shall not include any specific information relative to the
5 nature of the risk that is potentially exploitable.

6 (2) Prioritization of vulnerabilities.

7 (3) Identification of relevant internal resources.

8 (4) Strategy for addressing and mitigating those vulnerabilities.

9 (h) Communication of assessment results shall be restricted to
10 only approved government employees and validated contractors.
11 Assessment results and related aggregated reports shall be
12 confidential and, pursuant to Section 6254.19, shall be exempt
13 from disclosure under the California Public Records Act (Chapter
14 3.5 (commencing with Section 6250) of Division 7 of Title 1).

15 (i) Data produced by assessments shall be retained by all parties
16 for no longer than one year, unless the Governor's Office of
17 Emergency Services determines that retention for a longer period
18 is necessary.

19 SEC. 2. The Legislature finds and declares that Section 1 of
20 this act, which amends Section 11549.3 of the Government Code,
21 imposes a limitation on the public's right of access to the meetings
22 of public bodies or the writings of public officials and agencies
23 within the meaning of Section 3 of Article I of the California
24 Constitution. Pursuant to that constitutional provision, the
25 Legislature makes the following findings to demonstrate the interest
26 protected by this limitation and the need for protecting that
27 interest:

28 The state has a very strong interest in protecting its information
29 technology systems from intrusion, because those systems play a
30 critical role in assisting the entities of state government in carrying
31 out their duties. Thus, information regarding the specific
32 vulnerabilities of those systems should be protected at least until
33 those vulnerabilities have been remediated so as to preclude use
34 of that information to facilitate attacks on those systems.