BILL ANALYSIS

Department, Board, Or Commission	Author	Bill Number
Franchise Tax Board	**Hertzberg**	**SB 1444**

SUBJECT

State Agencies: Computerized Personal Information Security Plans

SUMMARY

This bill would require specified state agencies to develop a computerized personal information security plan.

REASON FOR THE BILL

The reason for the bill is to ensure that each state agency having specified personal information develops a computerized personal information security plan to mitigate and appropriately respond to a breach of the information.

EFFECTIVE/OPERATIVE DATE

This bill would become effective and operative January 1, 2017.

FEDERAL/STATE LAW

Federal law (Title III of Public Law 107-347) established the Federal Information Security Management Act of 2002 (FISMA). The National Institute of Standards and Technology (NIST) (a non-regulatory federal agency within the U.S. Department of Commerce) is responsible for FISMA implementation.

FISMA requires the development of information security standards and guidelines for non-national security federal information systems, including the development of:

- Standards to be used by federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels;
- Guidelines recommending the types of information and information systems to be included in each category; and
- Minimum information security requirements (management, operational, and technical security controls) for information and information systems in each such category.

State law (Government Code section 11549(a)) established the Office of Information Security (ISO) within the Department of Technology. The purpose of the ISO is to ensure 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.

Recently enacted legislation requires the ISO, in consultation with the Office of Emergency Services, to perform or require to be performed an independent security assessment of no fewer than 35 state agencies annually. The ISO is required to determine the basic standards of services to be performed as part of the independent security assessments.

State agencies and entities required to conduct or that receive an independent security assessment are required to transmit the complete results of that assessment and recommendations for mitigating system vulnerabilities, if any, to the ISO and the Office of Emergency Services.

Personal information is described in the California Civil Code sections 1798.3(a) and 1798.29(g) to mean:

- Any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual (1798.3(a)).
- An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted (1798.29(g)).
    - Social security number.
    - Driver's license number or California identification card number.
    - Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
    - Medical information.
    - Health insurance information.
    - Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.
- A user name or email address, in combination with a password or security question and answer that would permit access to an online account (1798.29(g)).

THIS BILL

This bill would require a state agency that owns or licenses computerized data that includes personal information to prepare a computerized personal information security plan that details the agency's strategy to respond to a security breach of computerized personal information and associated consequences caused by the disclosed personal information.

The computerized personal information security plan must include, but is not limited to, all of the following:

- A statement of the purpose and objectives for the plan.
- An inventory of the computerized personal information stored or transmitted by the agency.
- Identification of resources necessary to implement the plan.
- Identification of an incident response team tasked with mitigating and responding to a breach, or an imminent threat of a breach, to the security of computerized personal information.
- Procedures for communications within the incident response team and between the incident response team, other individuals within the agency, and individuals outside the agency that need to be notified in the event of a breach of the security of computerized personal information.
- Policies for training the incident response team and the agency on the implementation of the computerized personal information security plan, including, but not limited to, the use of practice drills.
- A process to review and improve the computerized personal information security plan.

For purposes of this bill, personal information would be described by reference to Sections 1798.3(a) and 1798.29(g) of the Civil Code (see the Federal/State Law section).

LEGISLATIVE HISTORY

AB 670 (Irwin, Chapter 518, Statutes of 2015) modified provisions of the independent security assessment program under the Office of Information Security to determine the basic standards of services to be performed as part of the independent security assessments and to conduct, or require to be conducted, an independent security assessment of every state agency, department, or office.

OTHER STATES' INFORMATION

Since this bill would require state agencies to develop a computerized personal information security plan, a review of other states' income tax laws is not relevant.

FISCAL IMPACT

This bill would not significantly impact the department's costs.

ECONOMIC IMPACT

This bill would not impact the state's income tax revenue.

APPOINTMENTS

None.

SUPPORT/OPPOSITION

Support: None on file.

Opposition: None on file.

VOTES

	Date	Yes	No
Assembly Floor	08/11/16	78	0
Senate Floor	05/31/16	39	0

LEGISLATIVE STAFF CONTACT

Contact	Work
Marybel Batjer, Agency Secretary, GovOps	916-651-9024
Khaim Morton, Legislative Deputy, GovOps	916-651-9100
Selvi Stanislaus, Executive Officer, FTB	916-845-4543
Gail Hall, Legislative Director, FTB	916-845-6333