

ANALYSIS OF AMENDED BILL

Author: Irwin Analyst: Janet Jennings Bill Number: AB 670
 Related Bills: None Telephone: 845-3495 Introduced and Amended Date: February 25, 2015, April 6, 2015
 Attorney: Bruce Langston Sponsor _____

SUBJECT:	State Agency Security Assessment
-----------------	----------------------------------

SUMMARY

This bill would, under the Government Code, modify provisions of the independent security assessment program under the Office of Information Security.

This analysis only addresses the provisions of the bill that impact the department's programs and operations.

RECOMMENDATION

No position.

Summary of Amendments

The bill as introduced February 25, 2015, and amended April 6, 2015, would modify the independent security assessment program, and allow the Governor's Office of Emergency Services to conduct the strategic direction of security assessments performed by the Military Department's Computer Network Defense Team, as specified.

Also, the amendments would:

- Restrict the communication of assessment results only to the assessed entity, approved government employees, and validated contractors.
- Require assessment results and relative aggregated reports to be confidential and exempt from disclosure by a Public Records Act request.
- Require data produced by assessments to be retained by all parties for no longer than one year, unless determined otherwise by the Governor's Office of Emergency Services.

This is the department's first analysis of the bill.

REASON FOR THE BILL

The reason for the bill is to improve security of the state's information technology.

EFFECTIVE/OPERATIVE DATE

This bill would become effective and operative January 1, 2016.

Board Position:	Executive Officer	Date
_____ S _____ NA <u> X </u> NP	Selvi Stanislaus	5/4/15
_____ SA _____ O _____ NAR		
_____ N _____ OUA _____		

FEDERAL/STATE LAW

Federal law established the Federal Information Security Management Act of 2002 (FISMA).¹ The National Institute of Standards and Technology (NIST) (a non-regulatory federal agency within the U.S. Department of Commerce) is responsible for the 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 established the Office of Information Security (Office) within the Department of Technology.² The purpose of the Office 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.

Current law allows the Office to conduct, or require to be conducted, independent security assessments of any state agency, department, or office, except the Department of Forestry and Fire Prevention, the cost of which is funded by the state agency, department, or office being assessed. The Office may require an audit of information security to ensure program compliance, the cost of which is funded by the state agency, department, or office being audited.

THIS BILL

This bill would require the Office to conduct, or require to be conducted, an independent security assessment of every state agency, department, or office, including the Department of Forestry and Fire Prevention, at least once every two years. The cost of the assessment is to be funded by the state agency, department, or office being assessed. The assessment results would be made available only to the assessed entity. The assessment must be conducted in compliance with the NIST Special Publication (SP) 800-53 controls, and to the extent practicable include:

- Vulnerability scanning, that includes, but is not limited to validation that (1) Information Technology systems have currently supported software, with all necessary security patches and updates applied, (2) security configurations are in compliance with NIST standards, (3) the network architecture is arranged to separate internal, publicly accessible and external zones, along with a mechanism to identify and alert on attempted intrusions.

¹ H. R. 2458-48.

² 11549 (a) of the Government Code.

- Penetration testing when determined appropriate by the Governor's Offices of Emergency Services.
- A report on the number, severity, and nature of identified vulnerabilities and recommendations for remediation and risk mitigation.

The bill would allow the Department of Technology to require any agency not in compliance with the above standards to redirect any funds within the agency's budget that may be legally expended for these purposes, for the purpose of paying the costs of compliance.

The bill would terminate the ability of the Office to require an audit of information security to ensure program compliance.

The Department of Technology would be required to adopt standards, specifying the manner for an assessed agency to communicate the assessment results to the Department of Technology that would include the following:

- Aggregated, statistical information relevant to the assessment results, including, but not limited to, the number of identified vulnerabilities categorized by high, medium, and low risk. These results would not include any specific information relative to the nature of the risk that is potentially exploitable.
- Prioritization of vulnerabilities.
- Identification of relevant internal resources.
- Strategy for addressing and mitigating those vulnerabilities.

The standards would be included in the State Administrative Manual.

The communication of assessment results would be restricted to approved government employees and validated contractors. Additionally, the results and related aggregated reports would be confidential and exempt from disclosure under the California Public Records Act.

The bill requires the data produced by the assessment to be retained by all parties for no longer than one year, unless the Governor's Office of Emergency Services determines that retention for a longer period is necessary.

IMPLEMENTATION CONSIDERATIONS

The FTB does not anticipate noncompliance issues related to an independent security assessment. However, if a deficit is found and the FTB is ordered to redirect funds, the redirection may interfere with the department's ability to establish business priorities and direction.

POLICY CONCERNS

The bill does not factor in a risk management process. NIST SP 800-53 states in part that information security considerations for information systems are examined in the context of an effective risk management process and not in isolation. The author may want to amend the bill to add a risk management process.

OTHER STATES' INFORMATION

Since this bill would set standards for independent security assessments of the state's information technology, a review of other states' income tax laws is not relevant.

FISCAL IMPACT

The FTB's costs to implement this bill have yet to be determined. The FTB has an established budget for annual security assessments of critical and/or high risk areas. To the extent that this bill would mandate a broader or more frequent security assessment and redirection of funds when such security assessments identify security compliance needs, there could be increased costs to the Department. As the bill moves through the legislative process, costs will be identified and an appropriation will be requested, if necessary.

ECONOMIC IMPACT

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

SUPPORT/OPPOSITION³

Support: RIMS.

Opposition: None on file.

ARGUMENTS

Proponents: Some may argue the state should have the same standards for information technology security assessments as the federal government.

Opponents: Some may argue that existing state law allows the Office to set standards to manage the state's information technology security and risk.

LEGISLATIVE STAFF CONTACT

Janet Jennings
Legislative Analyst, FTB
(916) 845-3495
janet.jennings@ftb.ca.gov

Jame Eiserman
Revenue Manager, FTB
(916) 845-7484
jame.eiserman@ftb.ca.gov

Gail Hall
Legislative Director, FTB
(916) 845-6333
gail.hall@ftb.ca.gov

³ According to the April 7, 2015, Assembly Committee on Privacy and Consumer Protection analysis.