STATE OF CALIFORNIA
Franchise Tax Board

Bill Analysis

Author: Irwin	Sponsor:	Bill Number: AB 869
	Related Bills: See Legislative History	Introduced: February 19, 2025

SUBJECT

State Agency Information Security Zero Trust Architecture

SUMMARY

This bill, under the Government Code (GOV) would require all state agencies to implement a "Zero Trust" cybersecurity architecture and require deadlines for various stages of implementation.

This analysis only addresses the provisions of the bill that would impact the Franchise Tax Board (FTB).

RECOMMENDATION

No position—The three-member Franchise Tax Board has not formally voted or taken a position on this bill.

SUMMARY OF AMENDMENTS

Not applicable.

REASON FOR THE BILL

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

ANALYSIS

This bill would require every state agency to implement Zero Trust architecture for all data, hardware, software, internal systems, and essential third-party software, including for on-premises, cloud, and hybrid environments, according to the following levels of maturity based upon the Cybersecurity and Infrastructure Security Agency (CISA) Maturity Model:

- Achieve "Advanced" maturity by June 1,2026.
- Achieve "Optimal" maturity by June 1, 2030.

This bill would require, in implementing Zero Trust architecture, state agencies to prioritize the use of solutions that comply with, are authorized by, or align to applicable federal guidelines, programs, and frameworks, including the Federal Risk and Authorization Management Program, the Continuous Diagnostics and Mitigation Program, and guidance and frameworks from the National Institute of Standards and Technology.

This bill would require implementation to, at a minimum, prioritize the following:

- Multifactor authentication for access to all systems and data owned, managed, maintained, or utilized by or on behalf of the state agency.
- Enterprise endpoint detection and response solutions to promote real-time detection of cybersecurity threats and rapid investigation and remediation capabilities.
- Robust logging practices to provide adequate data to support security investigations and proactive threat hunting.

This bill would require the Chief of the Office of Information Security (Chief) to develop or revise uniform technology policies, standards, and procedures for use by each state agency in implementing Zero Trust architecture to achieve the "Advanced" and "Optimal" maturity levels stated in the State Administrative Manual and Statewide Information Management Manual.

This bill would also require the Chief to update the requirements for existing annual reporting activities, including standards for audits and independent security assessments, to collect information relating to a state agency's progress in increasing internal defenses of agency systems, including:

- A description of any steps the state agency has completed, including advancements toward achieving Zero Trust architecture maturity levels.
- Following an independent security assessment, an identification of activities that have not yet been completed and that would have the most immediate security impact.
- A schedule to implement any planned activities.

This bill authorizes the Chief to update requirements for existing annual reporting activities, including standards for audits and independent security assessments, to also include information on how a state agency is progressing with respect to the following:

- Shifting away from trusted networks to implement security controls based on a presumption of compromise.
- Implementing principles of least privilege in administering information security programs.

- Limiting the ability of entities that cause cyberattacks to move laterally through or between a state agency's systems.
- Identifying cyber threats quickly.
- Isolating and removing unauthorized entities from state agencies' systems as quickly as practicable, accounting for cyber threat intelligence or law enforcement purposes.

This bill would provide the following definitions:

- "Chief" means the Chief of the Office of Information Security.
- "Cybersecurity and Infrastructure Security Agency (CISA) Maturity Model" means the Zero Trust Maturity Model published by the CISA.
- "Endpoint detection and response" means a cybersecurity solution that continuously monitors end-user devices to detect and respond to cyber threats.
- "Multifactor authentication" means using two or more different types of identification factors to authenticate a user's identity for the purpose of accessing systems and data.
- "State agency" has the same meaning as in GOV Section 11000.
- "Zero Trust architecture" means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy that employs continuous monitoring, risk-based access controls, secure identity and access management practices, and system security automation techniques to address the cybersecurity risk from threats inside and outside traditional network boundaries.

This bill would apply to the University of California only if the Regents of the University of California, by resolution, make any of these provisions applicable to the university.

Effective/Operative Date

This bill would be effective and operative January 1, 2026.

Federal/State Law

Federal Law

In 2002, the Federal Information Security Management Act (FISMA) was enacted, which mandated federal agencies provide security protections that were equal to the risk associated with an unauthorized disclosure of information maintained or collected by each federal agency. This requirement was extended to contractors working on behalf of a federal agency. In addition, FISMA requires federal agencies to meet the standards and guidelines established by the National Institute of Standards and Technology (NIST). NIST is a non-regulatory federal agency within the U.S. Department of Commerce and is charged with the implementation of FISMA. Zero trust

architecture was developed by NIST in 2020 and details authorization and authentication systems that are separate and distinct processes which prioritize protecting enterprise resources.

State Law

Currently the California Office of Information Security requires specified agencies, including FTB, to adopt and implement information security and privacy policies, standards, and procedures that adhere to NIST, the various Federal Information Processing Standards (FIPS) and perform a comprehensive, independent security assessment every two years. As an alternative, FTB may provide an annual declaration to the Chief of the Office of Information Security confirming that FTB has voluntarily and fully complied with the provisions in GOV section 11549.3(b) and (c), to be submitted by January 15 of each year.

Implementation Considerations

This bill would require changes to the department's network infrastructure, identity and access management systems, and FTB's enterprise data to revenue (EDR2) project. The requirements may interfere with existing enterprise-wide project timelines and the FTB may not have adequate time to implement all necessary changes without significant impacts and risks to the department. In light of these considerations, the author may wish to amend the bill to provide an exception for the FTB or to allow a delay in implementation pending completion of current FTB projects.

Technical Considerations

None noted.

Policy Considerations

None noted.

LEGISLATIVE HISTORY

AB 749 (Irwin, 2023/2024), similar to this bill, would have required all state agencies to implement a "Zero Trust" cybersecurity architecture and require deadlines for various stages of implementation. AB 749 was held by the Assembly Appropriation Committee without further action.

AB 2135 (Irwin, Chapter 773, Statutes of 2022) requires state agencies, as defined, to adopt and implement certain information security and privacy policies, standards, and procedures meeting specified federally established criteria; and requires those agencies to perform a comprehensive independent security assessment every two years, as specified.

AB 2623 (Gordon and Irwin, Chapter 389, Statutes of 2016) required specified state agencies to annually report to the Department of Technology a summary of the agency's actual and projected information security costs as specified.

PROGRAM BACKGROUND

Information received, generated, and maintained by the FTB is generally considered confidential unless specifically provided otherwise by statute. As a requirement for receiving Federal Taxpayer Information FTB has the additional responsibility of complying with the federal security requirements as specified by the NIST.

OTHER STATES' INFORMATION

None noted.

FISCAL IMPACT

The FTB's costs to implement this bill have yet to be determined. As the bill moves through the legislative process, costs will be determined.

ECONOMIC IMPACT

Revenue Estimate

This bill as introduced on February 19, 2025, would not impact state income or franchise tax revenue.

LEGAL IMPACT

None noted.

EQUITY IMPACT

None noted.

APPOINTMENTS

None noted.

SUPPORT/OPPOSITION

Assembly Floor analysis dated May 28, 2025.

Support

Microsoft Corporation

Opposition

None on file.

ARGUMENTS

Assembly Floor analysis dated May 28, 2025.

Proponents

This bill is supported by Microsoft Corporation and notes the following:

> On behalf of Microsoft, I am writing to express our strong support for Assembly Bill 869, which mandates the implementation of Zero Trust architecture for all state agencies to enhance cybersecurity measures. This bill is a significant step towards ensuring the security and integrity of California's digital infrastructure.
>
> AB 869 requires state agencies to prioritize solutions that comply with federal guidelines, programs, and frameworks, including multifactor authentication, enterprise endpoint detection and response solutions, and robust logging practices. These measures are crucial in protecting sensitive data and systems from cyber threats.
>
> Microsoft is committed to supporting the principles outlined in AB 869. We believe that the adoption of Zero Trust architecture will significantly improve the state's cybersecurity posture and help safeguard against potential vulnerabilities. Furthermore, we are prepared to offer our expertise and resources to assist state agencies in achieving the prescribed levels of maturity based on the Cybersecurity and Infrastructure Security Agency (CISA) Maturity Model.

Opponents

None on file.

LEGISLATIVE CONTACT

FTBLegislativeServices@ftb.ca.gov