SENATE COMMITTEE ON APPROPRIATIONS
Senator Anna Caballero, Chair
2025 - 2026 Regular Session

AB 869 (Irwin) - State agencies: information security: Zero Trust architecture

Version: February 19, 2025
Urgency: No
Hearing Date: August 18, 2025
Policy Vote: G.O. 15 - 0
Mandate: No
Consultant: Janelle Miyashiro

Bill Summary: AB 869 requires all California state agencies to implement Zero Trust architecture (ZTA) for all data, hardware, software, internal systems, and essential third-party software to achieve prescribed levels of maturity based on the Cybersecurity and Infrastructure Security Agency (CISA) Maturity Model, as specified. AB 869 also requires the Office of Information Security (OIS) to develop or revise uniform technology policies, standards, and procedures for use by each state agency in implementing ZTA to achieve the "Advanced" and "Optimal" maturity, as specified.

Fiscal Impact:
- The California Department of Technology (CDT), which houses OIS, reports the need for 7.0 permanent positions and costs of approximately $3.1 million in year one, $2.8 million in year two, $2.2 million in year three, and $1.9 million in year four and annually ongoing (General Fund). Costs to CDT include workload to implement and maintain the required ZTA, develop policy and technical standards and procedures, and implement statewide multi-factor authentication, endpoint protections, and increased logging practices.

- Unknown significant one-time and ongoing costs, ranging in the high hundreds of millions of dollars, for state agencies to implement ZTA (General Fund and various special funds). Actual costs to each impacted agency and department will depend on, among other things, the extent they may absorb this workload or other IT expenses within existing resources. See Staff Comments for additional detail.

Background: According to the National Institute of Standards and Technology (NIST), zero trust is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location. Zero trust focuses on protecting resources.

NIST defines a ZTA as an enterprise's cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan. The goal of a ZTA is to prevent unauthorized access to data and services while making the access control enforcement as granular as possible.

CDT issued a Technology Letter (23-01) "Multi-Factor Authentication Standard." Technology Letters (TL) are issued by the CDT to convey official communications regarding state IT, announce new (or changes to existing) IT policies and procedures,

or announce new (or changes to existing) state IT services or standards. TL 23-01 while announcing Statewide Information Management Manual (SIMM) 5360-C and 5360-D, which outlines standards for when and how to use multifactor authentication (MFA), also noticed the Administration's adoption of ZTA:

> This TL also serves as a notice that all State entities must work toward a Zero Trust Architecture (ZTA) model as outlined in NIST 800-207. Refer to the Cybersecurity Infrastructure Security Agency (CISA) Zero Trust Maturity Model Version 2.0. By May 2024, all State agencies/entities must have assessed, planned, and implemented the "Initial" maturity stage of each of the five pillars including Identity, Devices, Networks, Applications & Workloads, and Data.

Proposed Law:

- Requires every state agency to implement ZTA 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 CISA Maturity Model:
    - Achieve "Advanced" maturity by June 1, 2026.
    - Achieve "Optimal" maturity by June 1, 2030.

- Requires a state agency, in implementing ZTA, 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.

- Requires implementation to prioritize, at a minimum, 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.

- Requires the Chief of OIS, to develop or revise uniform technology policies, standards, and procedures for use by each state agency in implementing ZTA to achieve the "Advanced" and "Optimal" maturity levels stated in the State Administrative Manual (SAM) and Statewide Information Management Manual (SIMM), as specified, and authorizes a state agency to, but does not required, utilize the policies, standards, and procedures developed by the Chief of OIS, as specified.

- Requires the Chief of OIS to update 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 the internal defenses of agency systems, including:
    - A description of any steps the state agency has completed, including advancements toward achieving ZTA maturity levels.

  - Following and independent security assessment, and 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.

- Authorizes the Chief of OIS 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.

- Specifies that this bill applies to the University of California (UC) only to the extent that the Regents of the UC, by resolution, make any of these provisions applicable to the university.

- States that it is the intent of the Legislature that this bill be implemented in a manner that is consistent with the state's timely guidance with requirements that are conditions to receipt of federal funds, including, but not limited to, funding from the Infrastructure Investment and Jobs Act (IIJA), as specified.

- Defines, among other terms, "endpoint detection and response" to mean a cybersecurity solution that continuously monitors end-user devices to detect and respond to cyber threats.

- Defines, among other terms, "multifactor authentication" to mean using two or more different types of identification factors to authenticate a user's identity for the purposes of accessing systems and data.

- Defines, among other terms, "Zero Trust architecture" to mean 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.

- States legislative intent that the provisions of this bill be implemented in a manner that is consistent with the state's timely compliance with requirements that are conditions to receipt of federal funds, including, but not limited to, funding from the Infrastructure Investment and Jobs Act.

- States legislative findings and declarations.

Related Legislation: AB 979 (Irwin, 2025) requires, by July 1, 2026, the California Cybersecurity Integration Center (Cal-CSIC) to develop a California Artificial Intelligence (AI) Cybersecurity Collaboration Playbook to facilitate information sharing across the AI community and to strengthen collective cyber defenses against emerging threats. AB 979 is pending in this committee.

Staff Comments: While the total fiscal impact of the bill is unknown at this time, it will be significant and likely total into the high hundreds of millions of dollars. While not all state agencies would require the same level of resources, costs are anticipated to be significant for all impacted entities. Each agency and department operates with distinct processes and procedures, so resource requirements to implement the provisions of this bill are anticipated to vary greatly depending on the entity's size, operational scope, level of exposure through shared networks, and threat assessment, among other factors.

For context, below is a sample of state entities and their anticipated costs for additional staff, IT procurement, and other resource needs, as well as for workload for various activities to comply with the mandates of this bill:

- Entities within the California Health and Human Services Agency:
    - Department of Developmental Services: $7.2 million in Fiscal Year (FY) 2025-26 and $6.1 million in FY 2026-27 and annually ongoing (General Fund and federal funds).
    - Department of Health Care Services: $69 million over three FYs (General Fund and federal funds).
    - Department of Aging: Initial start-up costs of approximately $16.3 million and ongoing costs of $9.27 million (General Fund).
    - Department of Community Services and Development: One-time costs in the range of $1.6 million to $1.8 million and ongoing costs in the range of $1.4 million to $1.6 million (General Fund)
    - Department of Child Support Services: One-time cost in the range of $18 million to $24 million, and ongoing costs in the range of $9 million to $15 million (General Fund and federal funds).
    - Department of Managed Health Care: Annual ongoing costs of $10 million or more (Managed Care Fund).
    - Department of Rehabilitation: Total first year costs of approximately $31.3 million and ongoing costs of $21.3 million (General Fund).
    - Emergency Medical Services Authority: One-time cost in the range of $5 million to $15 million and ongoing costs ranging from $1.5 million to $5 million (General Fund). EMSA notes these costs are associated only with the EMS system, and do not include independently managed and sourced EMS systems throughout the state.
    - Department of Health Care Access and Information: One-time cost of $17.2 million and $1.8 million ongoing (General Fund).

- Entities within the Business, Consumer Services, and Housing Agency:
    - Department of Consumer Affairs: Total IT impact of approximately $20 million through FY 2030 (various special funds).
    - Department of Alcoholic Beverage Control: Costs in the range of $250,000 to $350,000 (Alcohol Beverage Control Fund).

  - Civil Rights Department: $718,000 in FY 2026-27 and $552,000 in FY 2027-28 and annually ongoing (General Fund).
  - Department of Real Estate: $386,000 in FY 2025-26, $378,000 in FY 2026-27 and FY 2027-28, $363,000 in FY 2028-29 and FY 2029-30, and $238,000 annually ongoing (Real Estate Fund).
  - Governor's Office of Business and Economic Development: One-time costs of $150,000 and $771,000 annually ongoing (General Fund).

- Entities within the California Environmental Protection Agency:
  - Department of Pesticide Regulation: One-time cost of approximately $1.45 million and total ongoing costs of $1.39 million (DPR Fund).
  - Department of Toxic Substances Control: $8.78 million annually from FY 2026-27 through FY 2029-30 and $7.03 million ongoing thereafter. DTSC notes increases in both the G&H Fee and the Environmental Fee by 4 percent would be required to support the costs associated with the bill.
  - Office of Environmental Health Hazard Assessment: Ongoing costs of $850,000 (General Fund).

- The Government Operations Agency (GovOps) reports unknown costs, likely ranging in the tens of thousands of dollars. Entities within GovOps noted the following:
  - Franchise Tax Board: $88.11 million in FY 2026-27, $61.04 million in FY 2027-28, $69.18 million in FY 2028-29, $51.79 million in FY 2029-30, and $54.39 million in FY 2030-31 (General Fund).
  - Department of General Services: One-time costs in the range of $101.46 million to $151.03 million and ongoing annual costs of $6.14 million (General Fund and special fund).

- The Department of Justice: $21.7 million in FY 2025-26, $42.0 million in FY 2026-27, $39.9 million in FY 2027-28, $40.5 million in FY 2028-29, $37.0 million in FY 2029-30, $30.8 million in FY 2029-30, and $24.6 million annually ongoing (General Fund, Federal Trust Fund, and False Claims Act).

- The Department of Forestry and Fire Protection: $1.25 million in year one, $2.08 million in year two, and $2.07 million annually ongoing (General Fund).

- The Office of Emergency Services: $1.26 million one-time and annually ongoing (General Fund).

- The California Department of Insurance: $1.15 million in FY 2025-26, $2.28 million in FY 2026-27, and $2.19 million in FY 2027-28 and annually ongoing (Insurance Fund).

- The California Department of Food and Agriculture: $28.5 million in the first four years and ongoing costs of approximately $8.0 million (General Fund).

- The Gambling Control Commission: $454,000 in year one, $517,000 in year two, and $509,000 annually ongoing (Gambling Control Fund).

- The California Community Colleges Chancellor's Office reports costs in the tens of thousands of dollars (General Fund). However, the office notes that it is not subject to the Governor's authority, so would not be required to conform to OIS policies, standards, and procedures, which may provide some additional flexibility regarding implementation.

Staff notes that many of the impacted agencies are special funded and generally do not receive General Fund support. This bill will likely create significant new cost pressures that impact these entities' operating costs and may necessitate or accelerate the need for future regulatory or license fee increases. To the extent impacted special fund agencies cannot absorb costs to comply with the mandates of this bill, there will be General Fund cost pressures.

Additionally, given current priorities and existing capabilities and resources, it is unlikely that many state agencies would be able to meet the mandates of this bill in the timeline established.

-- END --