Date of Hearing:
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 869 (Irwin) – As Introduced February 19, 2025

SUBJECT: State agencies: information security: Zero Trust architecture

SYNOPSIS

This author-sponsored measure would require California state agencies under the direct authority of the Governor to adopt certain cybersecurity standards and methodologies outlined in President Biden's Executive Order (EO) 14028 on "Improving the Nation's Cybersecurity." In particular, it would require adoption of a "Zero Trust" model for the state's information technology security architecture. As its name implies, Zero Trust is a cybersecurity approach that authenticates and authorizes every interaction between a network and a user or device, on the "never trust, always verify" principle.

This bill would provide a specific timeline and steps to be taken in implementing Zero Trust architecture at covered state agencies. Given the ever-growing danger of cyberattacks from both recognized threats, such as hackers, as well as unrecognized threats, such as trusted employees, adoption of Zero Trust will help ensure that state computer systems relied upon by millions of Californians will remain operational. The bill is virtually identical to AB 749 (Irwin, 2023), which passed this Committee on consent but was ultimately held on suspense in the Senate Appropriations Committee.

THIS BILL:

1) Makes the following findings and declarations:

    a) Recent cyber breaches have had wide-ranging consequences and demand a state-level response.

    b) Cyber defense requires greater speed and agility to mitigate cyber threats, limit the impact of data breaches, and better protect the state's workforce and residents.

    c) Cyberattacks not only significantly impact institutions financially, but they also erode public trust and confidence in government.

    d) To better defend against cyber threats, the Legislature intends for state agencies to embrace technologies and practices outlined in Executive Order 14028 on Improving the Nation's Cybersecurity. At a minimum, this includes formalizing Zero Trust as the desired model for security.

    e) Zero Trust is a security architecture requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or retaining access to applications and data.

2) Defines the following terms:

   a) "Chief" means the Chief of the Office of Information Security.

   b) "Endpoint detection and response" means a cybersecurity solution that continuously monitors end-user devices to detect and respond to cyber threats.

   c) "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.

   d) "State agency" means every state office, officer, department, division, bureau, board, and commission, excluding the California State University.

   e) "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.

3) Requires every state agency to implement Zero Trust architecture, including the following for all data, hardware, software, internal systems, and essential third-party software, including for on-premises, cloud, and hybrid environments:

   a) Multifactor authentication for access to all systems and data owned, managed, maintained, or utilized by or on behalf of the state agency.

   b) Enterprise endpoint detection and response solutions to promote real-time detection of cybersecurity threats and rapid investigation and remediation capabilities.

   c) Robust logging practices to provide adequate data to support security investigations and proactive threat hunting.

4) Directs state agencies, in implementing Zero Trust architecture, including multifactor authentication, 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.

5) Requires the 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, including multifactor authentication, on all systems in the State Administrative Manual and Statewide Information Management Manual.

6) Encourages, but does not mandate, state constitutional officers other than the Governor to use the policies, standards, and procedures developed by the Chief.

7) Requires the Chief 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) A description of any steps the state agency has completed, including advancements toward achieving Zero Trust architecture requirements and multifactor authentication.

b) Following an independent security assessment, an identification of activities that have not yet been completed and that would have the most immediate security impact.

c) A schedule to implement any planned activities.

8) Permits 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:

a) Shifting away from trusted networks to implement security controls based on a presumption of compromise.

b) Implementing principles of least privilege in administering information security programs.

c) Limiting the ability of entities that cause cyberattacks to move laterally through or between a state agency's systems.

d) Identifying cyber threats quickly.

e) Isolating and removing unauthorized entities from state agencies' systems as quickly as practicable, accounting for cyber threat intelligence or law enforcement purposes.

EXISTING LAW:

1) Establishes the California Department of Technology (CDT) in the Government Operations Agency (GovOps). (Gov. Code § 11545.)

2) Establishes the Office of Information Security (OIS) within CDT 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. (Gov. Code § 11549.)

3) Requires the Chief of OIS to establish an information security program with responsibilities including, among others, the creation, updating, maintenance, and issuing of information security and privacy policies, standards, and procedures for state agencies, and of policies, standards, and procedures directing state agencies to effectively manage security and risk for IT, and for mission critical, confidential, sensitive, or personal information. (Gov. Code § 11549.3(a).)

4) Requires state agencies and state entities within the executive branch that are under the direct authority of the Governor to implement the policies and procedures issued by OIS, as specified. (Gov. Code § 11549.3(b).)

5) Establishes information security and privacy policies, standards, and procedures for state entities within the executive branch that are not under the direct authority of the Governor. (Gov. Code § 11549.3(f).)

6) Establishes comprehensive information security and privacy policies, standards, and procedures for state agencies, including guidelines for risk management and assessment. (State Administrative Manual § 5300 et seq.)

7) Establishes standards, instructions, forms and templates that state agencies must use to comply with state information technology policy. (State Information Management Manual.)

COMMENTS:

1) **Author's statement**. According to the author:

> The cybersecurity of California's state agencies is foundational to the smooth and efficient operation of countless critical services. The State has a strong tradition of leveraging the expertise and example of our federal partners in the cybersecurity space to ensure Californians can have the same level of confidence in the security of their data and the dependability of services regardless of which level of government is responsible. Cybersecurity standards resulting from certain provisions of EO 14028 have already been adopted into California law. With AB 869 California will take an important step towards adoption of Zero Trust principles, by revising our standards and procedures to reflect them and put them into operation in already mandated processes, assessments, and reports.

2) **President Biden's Executive Order 14028 on "Improving the Nation's Cybersecurity."** EO 14028, dated May 12, 2021, opens with the following policy statement:

> The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. […]
>
> It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security. The Federal Government must lead by example. All Federal Information Systems should meet or exceed the standards and requirements for cybersecurity set forth in and issued pursuant to this order. (86 Fed. Reg. 26633.)

The EO goes on to set forth a detailed plan of action to strengthen federal cybersecurity on a prescribed timeline. While the EO is in many ways specific to the operations of the federal government, it endorses practices that, if applied in California, would enhance the state's cybersecurity. The EO outlines the following steps that this bill would require California state agencies to implement:

- "[D]evelop a plan to implement Zero Trust Architecture." (86 Fed. Reg. 26636.)
- "[E]mploy all appropriate resources and authorities to maximize the early detection of cybersecurity vulnerabilities and incidents on [government] networks." (86 Fed. Reg. 26643.)

- "[D]eploy an Endpoint Detection and Response (EDR) initiative to support proactive detection of cybersecurity incidents." (*Ibid.*)

- Capturing and maintaining "[i]nformation from network and system logs…[which is] invaluable for both investigation and remediation purposes." (86 Fed. Reg. 26644.)

3) **What this bill would do.** Under this bill, covered state entities would be required to implement Zero Trust architecture, which includes implementing the following:

- "Multifactor authentication for access to all systems and data owned, managed, maintained, or utilized by or on behalf of the state agency."

Multifactor authentication, at its most basic, means not permitting a user to log in to a network unless they can present more than one form of authentication to prove their identity. It is not sufficient for a user to simply enter their password in order to gain network access. Users will likely be regularly prompted to reauthenticate themselves in order to maintain network access.

- "Enterprise endpoint detection and response solutions to promote real-time detection of cybersecurity threats and rapid investigation and remediation capabilities."

A cybersecurity threat might involve a virus or malware infecting computers on the network. But it might also take the form of a trusted employee accessing files they do not ordinarily access, or downloading terabytes of data to a USB drive, in either case to purloin confidential or sensitive information. The phrase "enterprise endpoint detection and response" means continuously monitoring users' devices. The phrase "real-time detection of cybersecurity threats" means identifying such threats while they are occurring, rather than—as often occurs now—after the network has been hacked, when it is too late to prevent or mitigate the problem. In other words, this provision of the bill would require state agencies to use technologies to continuously monitor users' behavior and activity within their networks in order to rapidly (and ideally, immediately) identify threats as they occur.

- "Robust logging practices to provide adequate data to support security investigations and proactive threat hunting."

"Logging" means maintaining records of relevant activity in the network. This provision is meant to ensure that in the event of a successful cyberattack, there is sufficient, adequate information available to perform a forensic analysis meant to prevent a similar attack from occurring again.

In order to implement these requirements, the bill would require the state Office of Information Security (OIS) to update policies, standards, and procedures in the State Administrative Manual (SAM) and Statewide Information Management Manual (SIMM) to use in implementing Zero Trust architecture. State entities covered by the SAM and SIMM would have to include progress towards Zero Trust in their annual reporting, and the OIS would be free to update reporting requirements as necessary.

Entities deemed "constitutional officers"—i.e., those executive branch officers provided for under the California Constitution that are not under the direct authority of the Governor—including the Lieutenant Governor, Attorney General, Controller, Insurance Commissioner, Public Utilities Commission, Secretary of State, Superintendent of Public Instruction, Treasurer,

the State Board of Equalization, and the State Auditor, are not required to comply with the policies, standards, and procedures in the SAM and SIMM. Accordingly, this bill would provide these entities the option of using the updated policies, standards, and procedures therein.

4) **The urgency of improving the state's cybersecurity practices.** In 2021, the Newsom Administration, through the California Department of Technology, published *Cal-SECURE: State of California Executive Branch Multi-Year Information Security Maturity Roadmap* (Cal-SECURE),[1] which charts out a phased order of priority for cybersecurity capabilities, which includes many operational elements of Zero Trust architecture, including "privileged access management," "multifactor authentication," "mobile device management," "identity lifecycle management," "network threat detection," and "log management."[2] However, unlike EO 14028, Cal-SECURE does not provide a specific timeline for implementing these elements.

This bill would provide a definite timeline and steps to be taken in implementing Zero Trust architecture at state agencies. This is critical. Cybersecurity threats are present and growing. Postponing security measures that both the Biden and Newsom Administrations have recognized as important seems inadvisable. Moreover, this bill would make clear the importance of Zero Trust to constitutional officers and potentially encourage the architecture's adoption by those entities. As the author notes, the bill's benefits very likely outweigh its costs:

> Implementing multi-factor authentication, endpoint detection, and increasing logging practice would have associated costs, but would not prevent or significantly modify an agency's workflow. These capabilities would likely pay for themselves in avoided costs related to a potential breach or shutdown of an agency's systems.

Cybersecurity is ultimately not an abstract issue. The state operates critical computer systems related to public health (Covered California, MediCal), food assistance (CalFresh), labor and workforce development (unemployment insurance, workers' compensation), occupational licensing, and so forth. These systems are also replete with personal information. If these systems were disabled or malfunctioned due to a cyberattack, millions of vulnerable Californians and their families could be harmed.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file.

Opposition

None on file

Analysis Prepared by: John Bennett / P. & C.P. / (916) 319-2200

---

[1] Available at https://cdt.ca.gov/wp-content/uploads/2021/10/Cybersecurity_Strategy_Plan_FINAL.pdf.
[2] *Id.* at p. 10.