Date of Hearing: April 19, 2023

ASSEMBLY COMMITTEE ON ACCOUNTABILITY AND ADMINISTRATIVE REVIEW
Cottie Petrie-Norris, Chair
AB 749 (Irwin) – As Amended April 13, 2023

SUBJECT: State agencies: information security: uniform standards

DOUBLE REFERRAL: AB 749 (as amended March 14, 2023) was heard March 21, 2023, by the Assembly Committee on Privacy and Consumer Protection and was approved 11-0.

SUMMARY: Requires every state agency to implement Zero Trust architecture by January 1, 2026, including multifactor authentication, enterprise endpoint detection and response solutions, and robust logging practices, following uniform technology policies, standards, and procedures developed by the Chief of the Office of Information Security. Specifically, **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) Cyber attacks 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 within the California Department of Technology ("CDT").

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, by January 1, 2026, 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, no later than January 1, 2025, the Chief to develop uniform technology policies, standards, and procedures for use by each state agency in implementing Zero Trust architecture, 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 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 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.)

FISCAL EFFECT: Unknown. This bill has not been analyzed by a fiscal committee.

COMMENTS:

1) Background. The basic problem addressed by this bill is that traditional approaches to cybersecurity fail to address current and emerging threats to government networks. Such traditional approaches include securing the perimeter of a network with one or more firewalls, and requiring a user or device to submit a credential, such as a password, in order to gain access to a network. Once the user or device meets these requirements, that user or device is presumed to be trustworthy and generally need not demonstrate its trustworthiness again while logged into the network. It is well-known that hackers try, and sometimes succeed, in fraudulently meeting

these requirements through tactics such as phishing (posing as a trusted individual or entity in order to obtain passwords or other sensitive information). However, it is also disturbingly common for individuals who are in positions of trust, including employees and executives, to use legitimate network access in order to steal and reveal secure information.

In response, this bill proposes to require California state agencies to adopt certain cybersecurity standards and methodologies outlined in President Biden's Executive Order ("EO") 14028 on Improving the Nation's Cybersecurity, (86 Fed. Reg. 26,633 (May 17, 2021), available at https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.)

Foremost among these standards and methodologies is the adoption of a "Zero Trust" model for California state government's security architecture. As its name implies, Zero Trust, described in greater detail below, is a "cybersecurity approach that authenticates and authorizes every interaction between a network and a user or device—in contrast to traditional cybersecurity models that allow users or devices to move freely within the network once they are granted access. [Zero Trust architecture] works on the 'never trust, always verify' principle and assumes that attacks will come from within and outside of the network." (United States Government Accountability Office, *Science & Tech Spotlight: Zero Trust Architecture* (Nov. 18, 2022) GAO23-106065, available at https://www.gao.gov/products/gao-23-106065.)

2) 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. It is important to continue to identify and pursue additional elements of this EO and other work being done by [the National Institute of Standards and Technology (NIST)] and [the Cybersecurity and Infrastructure Security Agency (CISA)] to ensure we are continuing to follow cybersecurity best practices. With AB 749, 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."

3) Federal Executive Order. 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.)

4) What this bill would do. Under this bill, covered state entities would be required to implement Zero Trust architecture by January 1, 2026, 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 Chief 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.

5) Analysis of the need for this bill. 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"), which can be found at https://cdt.ca.gov/wp-content/uploads/2021/10/Cybersecurity_Strategy_Plan_FINAL.pdf. Cal-SECURE 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." (Cal-SECURE 7.) 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. It is inadvisable to postpone adopting security measures that both the Biden and Newsom Administrations have recognized the importance of. Moreover, this bill would make clear the importance of Zero Trust to constitutional officers and potentially encourage the architecture's adoption by those entities.

In addition, as the author notes, cost-benefit analysis likely favors this bill's adoption:

> "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. If these systems were disabled or malfunctioned due to a cyber attack, millions of vulnerable Californians and their families could be harmed.

6) Alignment to draw federal funds. According to the author, the Zero Trust architecture this bill would require aligns with cybersecurity provisions in the federal Infrastructure, Investment, and Jobs Act ("IIJA") and therefore will help position California to draw federal IIJA funds. Among the many IIJA programs is the State and Local Cybersecurity Grant Program ("SLCGP"), which requires each state to establish a cybersecurity committee and submit a cybersecurity plan, which currently is due September 30, 2023. California has already received about $8 million in SLCGP planning funds. The California Office of Emergency Services ("CalOES") is leading coordination of the planning committee. States will be required to demonstrate progress in implementing the plan for future rounds of funding. Moreover, other IIJA programs, such as funding for broadband infrastructure, include cybersecurity compliance elements.[1]

Recent amendments to this bill moved the date for the Chief to issue guidelines for Zero Trust architecture to January 1, 2025, and the date for state agencies to implement Zero Trust architecture to January 1, 2026. It is unclear if these dates are adequately aligned with individual IIJA program expenditure deadlines. For example, will these dates ensure compliance with cybersecurity provisions in IIJA broadband programs that require states to encumber funds by December 31, 2024, and spend them by December 31, 2026?

This bill would require state agencies, in implementing Zero Trust architecture, 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." It is unclear if this directive will ensure California is in compliance with cybersecurity elements of various IIJA programs, especially when each IIJA program has a Notice of Funding Opportunity and related conditions for funding that could still evolve.

Thus, both timing and substance of California's implementation of Zero Trust architecture could impact the state's ability to draw potentially billions of dollars in IIJA funds. Adequate flexibility in state statute to meet federal requirements is critical. Especially in times of budget deficits, it is good policy to position the state to maximize all federal funding opportunities. Accordingly, ***the committee may wish to consider amending the bill to express legislative intent that the state implement this bill in a manner that ensures timely compliance with requirements for federal funding, including, but not limited to, IIJA funding***.

ARGUMENTS IN SUPPORT:

BSA, the Software Alliance, an advocate for the global software industry, states: "We strongly encourage policymakers to support increased investment in modern IT infrastructure and cybersecurity, for example, by implementing zero trust architecture and using state-of-the-art identity, credentialing, and access management, which AB 749 proposes. Organizations, including governments, should expect these investments to grow as they continue their digital

[1] See, for example, the Notice of Funding Opportunity for the IIJA Broadband Equity, Access and Deployment program, available at BEAD NOFO.pdf (doc.gov) (at 70-71).

transformations, and thus are able to deliver better, more secure services to citizens and customers. This can be achieved by using commercial-off-the-shelf (COTS) solutions by enterprise technology companies who continuously update their solutions to improve both security and functionality."

RELATED LEGISLATION
AB 2135 (Irwin, Chap. 773, Stats. 2022) required state agencies not under direct authority of the Governor 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 2564 (Chau, 2020) would have stated the Legislature's intent to enact legislation to improve the security of information technology systems and connected devices by requiring public agencies and businesses to develop security vulnerability disclosure policies. The bill died without being referred to Committee.

REGISTERED SUPPORT / OPPOSITION:

Support

BSA the Software Alliance
Technology Industry Association of California

Opposition

None received

Analysis Prepared by: Jacqueline Kinney / A. & A.R. / (916) 319-3600