Date of Hearing: April 8, 2021

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 581 (Irwin) – As Amended March 25, 2021

SUBJECT: Cybersecurity

SUMMARY: This bill would require all state agencies to review and implement guidelines published by the National Institute of Standards and Technology (NIST), or derived therefrom, for reporting, coordinating, publishing, and receiving information about security vulnerabilities of state information technology (IT) systems and resolving those vulnerabilities. Specifically, **this bill would**:

1) Require all state agencies, as defined, to review and implement the NIST guidelines established pursuant to the Internet of Things Cybersecurity Improvement Act of 2020 (P.L. 116-207) no later than July 1, 2022, and specify that any state agency may elect to satisfy this requirement by implementing the standards and procedures published pursuant to 2), below.

2) Require the Chief of the Office of Information Security (OIS) to review the NIST guidelines established pursuant to the Internet of Things Cybersecurity Improvement Act, as specified, and create, update, and publish any appropriate standards or procedures in the State Administrative Manual and State Information Management Manual to apply the NIST guidelines to statewide governmental agencies no later than April 1, 2022.

3) Provide that, notwithstanding 1), above, a state entity, as defined, shall satisfy the requirement to implement guidelines as provided in 1) by implementing the standards and procedures established pursuant to 2).

4) Provide that, upon request by any state agency, OIS shall provide assistance in implementing the guidelines pursuant to 1) or 2), as applicable; and specify that a state agency may withdraw their request and discontinue any assistance from OIS at any time.

5) Provide that, upon request by any state agency, OIS and the California Cybersecurity Integration Center (CCIC) shall provide operational and technical assistance on reporting, coordinating, publishing, and receiving information about cybersecurity vulnerabilities of information systems; and specify that a state agency may withdraw their request and discontinue any operational or technical assistance from OIS or CCIC at any time.

EXISTING LAW:

1) Pursuant to the federal Internet of Things Cybersecurity Improvement Act of 2020 (P.L. 116-207, Stats. 2020), among other things, requires the Director of NIST, by June 2, 2021, in consultation with cybersecurity researchers and private sector industry experts, to develop and publish guidelines for the reporting, coordinating, publishing, and receiving of information about a security vulnerability relating to IT systems owned or controlled by a federal agency, including Internet of Things (IoT) devices owned or controlled by a federal agency, and the resolution of such a security vulnerability; and guidelines for a contractor providing an IT system to a federal agency, including an IoT device, and any subcontractor thereof, on receiving information about a potential security vulnerability relating to the IT

system, and disseminating information about the resolution of that security vulnerability. (15 U.S.C. Sec. 278g-3c(a).)

2) Specifies that the guidelines published pursuant to 1), above, shall align with industry best practices and standards established by the International Standards Organization, or any other appropriate, relevant, and widely-used standard, to the maximum extent practicable. (15 U.S.C. Sec. 278g-3c(b).)

3) Tasks the Director of the Office of Management and Budget (OMB) with overseeing the implementation of the guidelines published pursuant to 1), above, and, along with the Secretary of Homeland Security, providing operational and technical assistance in implementing the guidelines. (15 U.S.C. Sec. 278g-3c(d) and (e).)

4) Pursuant to state law, establishes, within the Government Operations Agency, the Department of Technology (CDT), and generally tasks the department with the approval and oversight of IT projects, and with improving the governance and implementation of IT by standardizing reporting relationships, roles, and responsibilities for setting IT priorities. (Gov. Code Sec. 11545, et seq.)

5) Establishes, within the CDT, the Office of Information Security (OIS), with the purpose of ensuring the confidentiality, integrity, and availability of state IT systems and promoting and protecting privacy as part of the development and operations of state IT systems, and tasks OIS with the duty to provide direction for information security and privacy to state government agencies, departments, and offices. (Gov. Code Sec. 11549(a) and (c).)

6) 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 Sec. 11549.3(a).)

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

8) Authorizes OIS to conduct, or require to be conducted, an independent security assessment (ISA) of every state agency, department, or office, the cost of which shall be funded by the state agency, department, or office being assessed, and specifies that OIS must, in consultation with the Office of Emergency Services, annually require no fewer than 35 state entities to perform an ISA. (Gov. Code Sec. 11549.3(c)(1) and (2).)

9) Authorizes the Military Department to perform an ISA of any state agency, department, or office, the cost of which shall be funded by the agency, department, or office being assessed. (Gov. Code Sec. 11549.3(c)(3).)

10) Requires state agencies and entities required to conduct or receive an ISA pursuant to 8), above, to transmit the complete results of that assessment and recommendations for mitigating system vulnerabilities, if any, to OIS and the Office of Emergency Services (Cal OES). (Gov. Code Sec. 11549.3(d).)

11) Defines "state agency" to include every state office, officer, department, division, bureau, board, and commission, except for the California State University. (Gov. Code Sec. 11000(a).)

12) Defines "state entity" to mean an entity within the executive branch that is under the direct authority of the Governor, including but not limited to, all departments boards, bureaus, commissions, councils, and offices, except the Transportation Agency, Department of Corrections and Rehabilitation, Department of Veterans Affairs, Business, Consumer Services, and Housing Agency, Natural Resources Agency, California Health and Human Services Agency, California Environmental Protection Agency, Labor and Workforce Development Agency, and Department of Food and Agriculture. (Gov. Code Sec. 11546.1(e)(2).)

13) Requires a manufacturer of a connected device, i.e. a device capable of connecting to the internet that is assigned an IP address or Bluetooth address, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification or disclosure. (Civ. Code Sec. 1798.91.04(a).)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of this bill**: This bill seeks to protect the personal information (PI) and critical infrastructure managed by the state's information technology systems by requiring state agencies to implement specified guidelines regarding the identification, reporting, and resolution of security vulnerabilities relating to information systems owned or controlled by state agencies. This bill is author sponsored.

2) **Author's statement**: According to the author:

> California lags behind federal efforts to have a uniform and efficient mechanism to receive, report, coordinate, and publish security vulnerabilities threatening the state. While the State has an internal tool to report known breaches and security incidents, the California Compliance and Security Incident Reporting System (Cal-CSIRS), this system does not provide advanced warning or guidance on how to resolve a security vulnerability that has yet to be exploited. The Cal-CSIC has numerous threat intelligence feeds from both commercial and public sources, including the Multi State Information Sharing and Analysis Center (MS-ISAC), Splunk, and Fireeye. However none of these services directly ingest information from state agencies, or allow for outside individuals to warn the Cal-CSIC about a vulnerability unique to the State or a particular state system. This leads to gap in California's understanding of our threat landscape and hinders our ability to proactively guard against threats.
>
> AB 581 requires state agencies to implement guidelines on the reporting, coordinating, publishing, and receiving of information related to security vulnerabilities of information systems published by NIST by July 1, 2022. This deadline is over a year after the statutory deadline for their publication, and 7 months after federal agencies must comply.

The bill also instructs CDT's Office of Information Security to adapt the NIST guidelines to statewide government agencies, make appropriate updates and additions to the State Administrative Manual (SAM) and State Information Management Manual (SIMM) by April 1, 2022, and provide assistance to agencies. This will give state agencies under the jurisdiction of CDT three months to adjust their implementation to published requirements in SAM and SIMM. Finally the Cal-CSIC is directed to give operational and technical assistance to agencies, as the key focusing point for state cybersecurity information sharing.

3) **State investments in cybersecurity**: Acknowledging the pressing cybersecurity issues facing this State and, in particular, the State's public agencies, California has in recent years invested heavily in the security of its IT infrastructure. In 2015, Executive Order B-34-15 required the Office of Emergency Services (Cal OES) to establish and lead the California Cybersecurity Integration Center (Cal-CSIC), with the primary mission to reduce the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, or public and private sector computer networks. The existence of Cal-CSIC was codified three years later by AB 2813 (Irwin, Ch. 768, Stats. 2018). In 2018, the Legislature passed AB 3075 (Berman, Ch. 241, Stats. 2018) which created the Office of Elections Cybersecurity within the Secretary of State, tasked with the primary mission to coordinate efforts between the Secretary of State and local elections officials to reduce the likelihood and severity of cyber incidents that could interfere with the security or integrity of elections. The Budget Act of 2020 (AB 89, Ting, Ch. 7, Stats. 2020) also made substantial investments in cybersecurity, including allocating $11.1 million to various departments to enhance the cybersecurity of the state's critical infrastructure, and $2.9 million to protect patient health records by strengthening cybersecurity throughout the state's public health infrastructure.

   In 2010, the Legislature passed AB 2408 (Smyth, Ch. 404, Stats. 2010), which, among other things, required the chief of OIS to establish an information security program, with responsibilities including 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 Sec. 11549.3(a).) AB 2408 provided that all state entities shall implement the policies and procedures issued by OIS, including compliance with its information security and privacy policies, standards, and procedures, and with filing and incident notification requirements. (Gov. Code Sec. 11549.3(b).) Five years later, the Legislature expanded on the authority of OIS by passing AB 670 (Irwin, Ch. 518, Stats. 2015), which authorized OIS to conduct, or require to be conducted, an ISA of every state agency, department, or office, at the expense of the entity being assessed, and specified that OIS must, in consultation Cal OES, annually require no fewer than 35 state entities to conduct an ISA. (Gov. Code Sec. 11549.3(c)(1) and (2).)

   Despite some shortcomings[1], these efforts have largely been successful at fortifying state cybersecurity. According to CDT's 2020 Information Technology Annual Report, CDT's Security Operations Center blocked roughly 200 million malicious probes daily, and processed over 12,000 threat events resulting in 240 security notifications to state entities to

[1] *See,* e.g., Elaine M. Howle, "Gaps in Oversight Contribute to Weaknesses in the State's Information Security: High Risk Update – Information Security," *Auditor of the State of California*, Report 2018-611, July 2019.

investigate and remediate threats.[2] These numerous threats resulted in only a single incident that led to the unauthorized disclosure of PI by a state entity.

Though these advances are laudable, California's state information security infrastructure still has significant room for improvement. The threat figures reported by CDT's Security Operations Center account only for security incidents that have been detected; unknown security vulnerabilities and undetected intrusions on state networks are obviously not reflected. Existing law requires regular ISAs to identify technical gaps in information security, but even the most thorough assessment by a single entity can miss critical vulnerabilities, particularly when considering the multitude of connected devices and software the state employs. As state agencies become increasingly reliant on IT systems of varied use and origin for day-to-day and public-facing operations, they face a growing collection of possible security vulnerabilities. These interconnected systems are ultimately only as secure as their weakest link, necessitating consistent protocols for identifying, and disseminating information about, security vulnerabilities as they are detected and before they can compromise critical systems.

This bill seeks to apply federal guidelines related to reporting and resolving security vulnerabilities to state agencies in order to strengthen the State's cyberdefense and protect both the considerable PI and the critical infrastructure that state IT supports.

4) **Internet of things (IoT), generally**: The internet of things (IoT), generally refers to the growing constellation of appliances, devices, and other goods with the capacity for interconnectivity either through the internet or through more local means of interface. As a 2014 Forbes article on the topic describes:

> Simply put, [the IoT] is the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other). This includes everything from cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig. [I]f it has an on and off switch then chances are it can be a part of the IoT. […] The IoT is a giant network of connected 'things' (which also includes people). The relationship will be between people-people, people-things, and things-things. […] On a broader scale, the IoT can be applied to things like transportation networks: 'smart cities' which can help us reduce waste and improve efficiency for things such as energy use; this helping us understand and improve how we work and live.[3]

Juniper Research, a technology market research and analytics consulting firm, estimates that the number of IoT devices in 2021 will reach 46 billion, a 200% increase from 2016, and by 2030, that number is expected to rise to over 125 billion. This meteoric rise in IoT does not come without risks. As the same 2014 Forbes article points out:

---

[2] "California Information Technology Annual Report 2020: Leadership in a Time of Crisis," *California Department of Technology*, 2021, p. 12.
[3] Jacob Morgan, Forbes, "A Simple Explanation of 'The Internet Of Things'", *Forbes*, May 13, 2014, https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/ [as of Apr. 3, 2021].)

> The reality is that the IoT allows for virtually endless opportunities and connections to take place, many of which we can't even think of or fully understand the impact of today. It's not hard to see how and why the IoT is such a hot topic today; it certainly opens the door to a lot of opportunities but also to many challenges. Security is a big issue that is oftentimes brought up. With billions of devices being connected together, what can people do to make sure that their information stays secure? Will someone be able to hack into your toaster and thereby get access to your entire network? The IoT also opens up companies all over the world to more security threats. Then we have the issue of privacy and data sharing.

A 2017 report by the U.S. Department of Justice (DOJ) Criminal Division's Cybersecurity Unit and the Consumer Technology Association advising IoT device owners on practices to institute when using most internet-connected devices, details the risks as follows:

> In recent years, the dramatic growth of Internet-connected devices has transformed how people, households, and businesses interact with each other and the physical world. Connected devices as diverse as security cameras, digital video recorders, printers, wearable devices, "smart" lightbulbs, and Internet connected-appliances have come to be collectively known as the "Internet of Things" ("IoT"). IoT devices represent a growing constellation of gadgets and tools designed to collect, exchange, and process information over the Internet to furnish their users with convenient access to an array of services and information.
>
> Unfortunately, IoT devices have also become an increasingly attractive target for criminals. To attack IoT devices, cyber criminals often probe the devices for security vulnerabilities and then install malicious software ("malware") to surreptitiously control the device, damage the device, gain unauthorized access to the data on the device, and/or otherwise affect the device's operation without permission. Installed malware may not only compromise the operation and information security of the infected IoT device, but can also provide hackers a conduit for penetrating other electronic devices on the same network. Unless appropriate precautions are taken, malware can quickly spread across networks of IoT devices without a user opening a file, clicking on a link, or doing anything other than turning on an Internet-connected device.
>
> Although malware has existed for many years, the burgeoning popularity of IoT devices has significantly increased the number of Internet-accessible targets that may be exploited; the advent of a new generation of malware dedicated to exploiting IoT devices is largely to blame.[4]

In 2018, California took a significant step toward addressing the risks associated with security vulnerabilities in IoT devices by passing SB 327 (Jackson, Ch. 886, Stats. 2018), which required manufacturers of connected devices to equip those devices with reasonable security features to protect the device and information therein from unauthorized access, destruction, use, modification, or disclosure. Though this supply-side approach to IoT cybersecurity requires consideration of cybersecurity in the design of IoT devices, many vulnerabilities are not identified until after these devices enter the market. Depending on

---

[4] "Securing Your 'Internet of Things' Devices," *U.S. DOJ Cybersecurity Unit*, Jul. 2017.

how the devices are being used at the time a vulnerability is exploited, the costs of overlooking such security weaknesses can be dire.

5) **The federal Internet of Things Cybersecurity Improvement Act of 2020**: Recognizing the potential risks presented by the rapidly expanding IoT infrastructure of the federal bureaucracy, in late 2020, Congress passed H.R. 1668, and the President signed into law, the bipartisan IoT Cybersecurity Improvement Act of 2020 (P.L. 116-207), which primarily required NIST to promulgate guidelines relating to the use and management of IoT devices, and to the reporting and resolution of security vulnerabilities identified with respect to those devices, as well as the adoption and implementation of those standards by all federal agencies.

   Specifically, the Act requires the Director of NIST, by June 2, 2021, in consultation with cybersecurity researchers and privacy sector industry experts, to develop and publish guidelines for the reporting, coordinating, publishing, and receiving of information about a security vulnerability relating to IT systems owned or controlled by a federal agency, including IoT devices, and the resolution of such a security vulnerability. The Act also required the Director of NIST to develop and publish guidelines for a contractor providing an IT system to a federal agency, including an IoT device, and any subcontractor thereof, on receiving information about potential security vulnerabilities relating to the IT system, and the dissemination of information about the resolution of that vulnerability.

   The Act specifies that these guidelines must align with industry best practices and standards established by the International Standards Organization, or another appropriate, relevant, and widely-used standard, to the maximum extent practicable, and that they must be consistent with the policies and procedures produced pursuant to the Homeland Security Act of 2002 and include guidelines on both of the following: receiving information about a potential security vulnerability relating to an information system owned or controlled by an agency (including an IoT device); and disseminating information about the resolution of a security vulnerability relating to an information system owned or controlled by an agency (including an IoT device). Finally, the Act tasks the Director of the OMB with overseeing the implementation of these guidelines and, along with the Security of Homeland Security, providing operational and technical assistance to agencies and contractors seeking to implement them.

   AB 581 would parallel the requirements of the IoT Cybersecurity Improvement Act at the state level, by requiring OIS to publish guidelines based on those developed by NIST, requiring all state agencies to adopt either the guidelines published by NIST or those published by OIS, and tasking OIS and the CCIC to, upon request of the agency, provide assistance with implementing the guidelines and provide operational and technical assistance, respectively.

6) **AB 581 would provide consistent standards for addressing security vulnerabilities across state agencies, while preserving independence of non-reporting entities**: AB 581 would require all state agencies to review and implement the NIST guidelines established pursuant to the IoT Cybersecurity Improvement Act of 2020, and would require the Chief of OIS to review those guidelines and create, update, and publish any appropriate standards or procedures in the State Administrative Manual (SAM) and State Information Management Manual (SIMM) to apply the NIST guidelines to statewide government agencies. The bill

would also require any state entity under the authority of the Governor (i.e., "reporting entities") to implement the standards and procedures published in accordance with the latter requirement (i.e. by the Chief of OIS), rather than the NIST standards as originally published. All agencies would be required to implement these guidelines by July 1, 2022 (just over one year after their scheduled publication), and the Chief would be required to produce their standards and procedures by April 1, 2022. Finally, the bill would require OIS to, upon an agency's request, assist state agencies in implementing these guidelines, and require the CCIC to, upon an agency's request, provide operational and technical assistance on developing their security vulnerability information systems. The bill makes clear that these services are elective, and that a state agency may withdraw their request for assistance, and discontinue assistance, from OIS or the CCIC at any time.

In effect, the result of this is that state agencies not under the direct authority of the Governor (i.e., "non-reporting entities") would be required to, at minimum, adopt the NIST guidelines as published, while all other state agencies (i.e., those under the Governor's authority) would be required to implement a modified version of those guidelines published by OIS that are adjusted to better suit their application to statewide agencies. This is intended to avoid the recurring concern of non-reporting agencies that requirements to comply with standards created by an agency under the Governor's control could interfere with the separation of powers, being used malevolently or strategically to coerce behavior by those agencies, which the state constitution intends to be independent. The bill has prudently been amended, however, to permit non-reporting entities to electively adopt the guidelines promulgated by OIS rather than the original NIST guidelines, should they so desire. Considering the OIS guidelines are, by design, likely to be better suited for the application to California's state agencies, it may in some circumstances be in the best interest of both the non-reporting entities and the State's cybersecurity interests for these agencies to adopt the OIS guidelines. Providing this option, while requiring only compliance with the federal standards, seems to strike the proper balance between ensuring consistent, high-quality security vulnerability reporting and resolution practices are adopted across state agencies, and preserving the independence of non-reporting entities from the authority of reporting entities, and, by extension, the Governor.

7) **NIST guidelines are not yet published, but sufficiency of forthcoming guidelines can be reasonably anticipated**: The IoT Cybersecurity Improvement Act of 2020 requires NIST to promulgate its guidelines relating to security vulnerability reporting and resolution no later than 180 days after the date of the enactment of the Act. (15 U.S.C. 278g-3c(a).) Because the Act went into effect on January 1, 2021, the deadline for publication of these guidelines is June 2, 2021, and as of the date of this bill's hearing, the guidelines have not yet been published.

   Non-reporting agencies would be obligated under this bill to comply with either the NIST guidelines themselves or the guidelines issued by OIS based on those guidelines, and, in order to maintain independence from the authority of the Governor, have typically resisted subjecting themselves to the policies or oversight of OIS. (*See* Comment 6.) Because the NIST guidelines upon which this bill is based are not yet available to review, stakeholder discussions have raised concerns among non-reporting agency representatives that the adequacy of the NIST guidelines for state purposes and their capacity to comply with the guidelines cannot be properly evaluated. These concerns have led some to suggest that the bill should be delayed until next year, when the guidelines will have been issued.

In response to these suggestions, the author points out that NIST's credibility for developing excellent standards with broad applicability should be sufficient to assume acceptability of the standards, even prior to publication. According to the author:

> […]NIST is a well-respected entity in cybersecurity and other STEM fields. It is a non-artisan entity that provides ample opportunities for peer-review and comment on the guidelines before they are published. NIST's cybersecurity guidelines in various areas have been widely adopted by both public and private sector actors, and are generally considered the gold-standard.
>
> While we may not know the exact details of the guidelines that will be delivered in June, they will not be controversial or partisan, and cybersecurity experts from all backgrounds will have had the opportunity to collaborate on them. We also have no time to waste in getting the ball rolling making changes to state agencies to enhance our cybersecurity capabilities. As SolarWinds and other successful attacks against state resources have proven time and time again, we are not preparing for "if"; we are actively responding to "how" and "what."

Staff notes that it is not uncommon for this Legislature to pass laws requiring compliance with guidelines or regulations that are yet to be promulgated, though typically the forthcoming regulations are to be developed by state, rather than federal, entities. Staff further notes that the deadline for NIST to issue these guidelines precedes the state's deadlines for the passage of bills out of the Legislature, and for approval by the Governor, by several months. As such, should this bill continue through the legislative process, it is likely that the guidelines will be available for review before the bill must be finally approved.

8) **Related legislation:** AB 809 (Irwin) would require state agencies that do not fall under the direct authority of the Governor to adopt and implement certain information security and privacy policies, standards, and procedures meeting specified federally-established criteria, and would require those agencies to perform a comprehensive ISA every two years for which they may contract with the Military Department.

   AB 1352 (Chau) would authorize the Military Department to perform an ISA of a local educational agency or schoolsite at the request and expense of the local educational agency.

9) **Prior legislation:** AB 89 (Ting, Ch. 7, Stats. 2020) *See* Comment 3.

   AB 2564 (Chau, 2020) stated the intent of the Legislature 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. This bill was never referred to a committee, and died at the Desk.

   AB 2669 (Irwin, 2020) was substantially similar to AB 809 (Irwin, 2021). This bill was not set for hearing in the Assembly Committee on Privacy and Consumer Protection.

   SB 327 (Jackson, Ch. 886, Stats. 2018) *See* Comment 4.

   AB 2813 (Irwin, Ch. 768, Stats. 2018) *See* Comment 3.

   AB 3075 (Berman, Ch. 241, Stats. 2018) *See* Comment 3.

AB 3193 (Chau, 2018) would have required all state agencies, including those not under the direct authority of the governor, to comply with the information security and privacy standards and practices established by OIS, and to undergo ISAs as required by OIS. This bill died in the Senate Governmental Organization Committee.

AB 670 (Irwin, Ch. 518, Stats. 2015) *See* Comment 3.

AB 1172 (Chau, 2015) would have continued the existence of the California Cyber Security Task Force created by Governor Brown within the Office of Emergency Services until 2020, to act in an advisory capacity and make policy recommendations on cybersecurity for the state, and would have created a State Director of Cyber Security position with specified duties within the Office of Emergency Services. This bill died on the Senate Inactive File.

AB 2408 (Smyth, Ch. 404, Stats. 2010) *See* Comment 3.

10) **Double referral**: This bill is double referred to the Assembly Committee on Accountability and Administrative Review.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

Analysis Prepared by: Landon Klein / P. & C.P. / (916) 319-2200