SENATE COMMITTEE ON GOVERNMENTAL ORGANIZATION
Senator Bill Dodd
Chair
2021 - 2022 Regular

Bill No:	AB 581	**Hearing Date:**	6/14/2022
Author:	Irwin		
Version:	6/8/2022 Amended		
Urgency:	No	**Fiscal:**	Yes
Consultant:	Brian Duke		

SUBJECT: Cybersecurity

DIGEST: This bill requires all state agencies to review and implement specified National Institute of Standards and Technology (NIST) guidelines for, among other things, reporting, coordinating, publishing, and receiving information about security vulnerabilities of state information technology (IT), as specified, and requires the Chief of the Office of Information Security (OIS) to review the NIST guidelines and to create, update, and publish appropriate standards, as specified.

ANALYSIS:

Existing law:

1) Establishes OIS, within the Department of Technology (DOT) and under direction of the Chief of OIS, 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 residence of the state.

2) Establishes the California Cybersecurity Integration Center (Cal-CSIC) with the primary mission of reducing the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks in the state.

3) Requires an entity within the executive branch that is under the direct authority of the Governor to implement the policies and procedures issued by the OIS.

4) Authorizes OIS to conduct, or require to be conducted, an independent security assessment of every state agency, department, or office, as specified.

5) Defines "state agency" to include every state office, officer, department, division, bureau, board, and commission. "State agency" does not include the California State University, as specified.

This bill:

1) Requires all state agencies to review and implement the NIST guidelines no later than July 1, 2023, as specified. A state agency's review and implementation of the guidelines may include modifying terms and structures applicable to federal entities to appropriately apply to a state agency, including establishing procedures for receiving vulnerability information and resolving reported vulnerabilities, as specified.

2) Requires the Chief of OIS to review the NIST guidelines 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 state agencies and state entities, no later than April 1, 2023.

3) Requires OIS, upon request by any state agency or state entity, to provide assistance in implementing the guidelines or the standards and procedures, as specified. A state agency may withdraw their request and discontinue any assistance from OIS at any time.

4) Requires OIS and the Cal-CSIC, upon request by any state agency or state entity, to provide operational and technical assistance on reporting, coordinating, publishing, and receiving information about cybersecurity vulnerabilities of information systems. A state agency may withdraw their request and discontinue any operations or technical assistance from OIS or Cal-CSIC at any time.

5) Includes legislative findings and declarations relating to cybersecurity.

Background

Purpose of the Bill. According to the author's office, "California has become a leader in many areas of cybersecurity among the states, including being a key resource for advice and aid when other states have had their information systems attacked. Nevertheless, California lags behind federal efforts to have a uniform and efficient mechanism to receive, report, coordinate, and publish security vulnerabilities threatening the State. With the Federal Government recently directing NIST to develop guidelines for vulnerability disclosure and remediation, California has the opportunity to indirectly benefit from these federal efforts. AB

581 will require California state agencies to adopt these NIST guidelines, so state systems and data will be more secure, will be more reliable, and provide Californians with the services and privacy they expect and deserve. As the state and public have increasingly relied on our shared digital infrastructure, it is now more important than ever to secure our state systems."

National Institute of Standards and Technology. The NIST was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. Congress established the agency to remove a major challenge to U.S. industrial competitiveness at the time – a second-rate measurement infrastructure that lagged behind the capabilities of the United Kingdom, Germany, and other economic rivals. From the smart electric power grid and electronic health records to atomic clocks, advanced nanomaterials and computer chips, innumerable products and services rely in some way on technology, measurement and standards provided by the NIST.

According to the NIST, reporting known or suspected security vulnerabilities in digital products is one of the best ways for developers and services to become aware of issues. Formalizing actions to accept, assess, and manage vulnerability disclosure reports can help reduce known security vulnerabilities. The 2021 Draft NIST Special Publication 800-216 *Recommendations for Federal Vulnerability Disclosure Guidelines* recommends guidance for establishing a federal vulnerability disclosure framework and highlights the importance of proper handling of vulnerability reports and communicating the minimization or elimination of vulnerabilities.

California's 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 2010, the Legislature passed AB 2408 (Smyth, Chapter 404, Statutes of 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.

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. Five years later, the Legislature expanded on the authority of OIS by passing AB 670 (Irwin, Chapter 518, Statutes of 2015), which

authorized OIS to conduct, or require to be conducted, an independent security assessment (ISA) of every state agency, department, or office. In 2015, Executive Order B-34-15 required the Office of Emergency Services (OES) to establish and lead the 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, Chapter 768, Statutes of 2018).

The internet of things (IoT), 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. A 2017 report by the United States 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:

> 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.

In 2018, California took a significant step toward addressing the risks associated with security vulnerabilities in IoT devices by passing SB 327 (Jackson, Chapter 886, Statutes of 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 devices enter the market. Depending on how the devices are being used when a vulnerability is exploited, the costs of overlooking such security weaknesses can be dire.

Recognizing the potential risks presented by the rapidly expanding IoT infrastructure of the federal bureaucracy, in late 2020, the President signed into law the bipartisan IoT Cybersecurity Improvement Act of 2020 (P.L. 116-207). The

Act required 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 specified 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 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). These guidelines were published in June 2021. Finally, the Act tasks the Director of the Office of Management and Budget (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.

This bill parallels the requirements of the IoT Cybersecurity Improvement Act at the state level. This bill requires all state agencies to review and implement the NIST guidelines established pursuant to the IoT Cybersecurity Improvement Act of 2020, and requires 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 state agencies. The bill also requires any state agency 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 are required to implement these guidelines by July 1, 2023 (just over one year after their scheduled publication), and the Chief is required to produce their standards and procedures by April 1, 2023. Finally, the bill requires OIS to, upon an agency's request, assist state agencies in implementing these guidelines, and requires the CAL-CSIC 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 CAL-CSIC 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 also permits 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.

In April 2021, though not opposed to the bill, State Treasurer Fiona Ma, along with Insurance Commissioner Ricardo Lara and Controller Betty Yee, expressed "concerns [that] the NIST guidelines are not yet finalized and expecting my office to commit to implementing yet to be finalized standards is very concerning. While I do not believe there will be anything nefarious in the forthcoming NIST standards, I would be more comfortable knowing my Chief Information Officer has been provided ample time to review and assess how the finalized guidelines will impact my office." As noted previously, NIST published the requisite guidelines in June 2021.

Prior/Related Legislation

SB 892 (Hurtado, 2022) requires OES to develop, propose, and adopt optional reporting guidelines for companies and cooperatives in the food and agriculture industry and entities in the water and wastewater systems industry if they identify a significant and verified cyber threat; and, requires OES and Cal-CSIC to prepare

and submit a multiyear outreach plan to assist those sectors in their efforts to improve cybersecurity and an evaluation of options for providing grants or alternative forms of funding in their efforts to improve cybersecurity preparedness, as specified. (Pending in the Assembly Emergency Management Committee)

AB 2135 (Irwin, 2022) requires 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 requires those agencies to perform a comprehensive ISA every two years for which they may contract with the Military Department or a qualified responsible vendor. (Pending in the Senate Governmental Organization Committee)

AB 2355 (Salas, 2022) requires any local education agency to report any cyberattack impacting more than 500 pupils or personnel to Cal-CSIC, as specified. (Pending in the Senate Governmental Organization Committee)

AB 2813 (Irwin, Chapter 768, Statutes of 2018) established Cal-CSIC in statute.

AB 670 (Irwin, Chapter 518, Statutes of 2015) authorized OIS to conduct, or require to be conducted, an ISA of every state agency, department, or office.

AB 2048 (Smyth, Chapter, Statutes of 2010) codified the Governor's Reorganization Plan No. 1 of 2009 which consolidated state IT functions under the Office of the State Chief Information Officer, as specified.

FISCAL EFFECT: Appropriation: No Fiscal Com.: Yes Local: No

SUPPORT:

Splunk, Inc.

OPPOSITION:

None received

ARGUMENTS IN SUPPORT: In support of the bill, Splunk, Inc. writes that, "California is a leader in data protection. The actions the state takes with regard to cybersecurity are important due to the need to defend the integrity of its own data and IT systems, and as a standard setter in global cybersecurity evolution. Information-sharing best practices, including coordinated vulnerability disclosure programs, are an integral component of a mature cybersecurity defense program.

With the passage of AB 581, California would join the U.S. federal government as an important adopter of systemic coordinated vulnerability disclosure programs."