ASSEMBLY THIRD READING
AB 581 (Irwin)
As Amended January 24, 2022
Majority vote

SUMMARY

This bill requires 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.

Major Provisions

1) Requires 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, 2023, and specifies that any state agency may satisfy this requirement by implementing the standards and procedures published pursuant to 2), below.

2) Requires 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 state agencies and state entities no later than April 1, 2023; provides that, notwithstanding 1), above, a state agency or state entity under the direct authority of the Governor shall satisfy the requirement to implement guidelines as provided in 1) by implementing these standards and procedures.

3) Provides that, upon request by any state agency or state entity, OIS shall provide assistance in implementing the guidelines pursuant to 1) or 2), as applicable, and OIS and the California Cybersecurity Integration Center (Cal-CSIC) shall provide operational and technical assistance on reporting, coordinating, publishing, and receiving information about cybersecurity vulnerabilities of information systems.

COMMENTS

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 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.

Though these advances are laudable, California's state information security infrastructure still has room for improvement. Existing law requires regular ISAs to identify gaps in information security, but even the most thorough assessment 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.

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 (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:

> [] 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.[1] 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.

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,

---

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-216-draft.pdf

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.[1]

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.

Arguments in Support

Splunk, Inc., a data-sharing software company based in San Francisco, argues:

> 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 [(CVD)], 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 systematic coordinated vulnerability disclosure programs.
>
> NIST is a respected cybersecurity standard setter, known for careful and thorough development of frameworks that help organizations understand and mitigate cybersecurity risks. NIST's current work on CVD best practices will become the standard for U.S. federal government CVD programs and is logical guidance for the State of California as it implements its own CVD programs.

Arguments in Opposition

None on file

FISCAL COMMENTS

According to the Assembly Appropriations Committee, "[c]osts (General Fund (GF)) in the millions of dollars for state agencies to review and implement NIST guidelines on IT security [and] [u]nknown, but possibly significant costs (GF) to the OIS at the California Department of Technology (CDT), possibly in the hundreds of thousands of dollars in increased staff workload to update the SAM and SIMM to apply NIST guidelines by **[]** and provide technical assistance to state agencies to comply with the updated regulations."

VOTES

ASM PRIVACY AND CONSUMER PROTECTION: 11-0-0
YES: Chau, Kiley, Bauer-Kahan, Bennett, Carrillo, Cunningham, Gabriel, Gallagher, Irwin, Lee, Wicks

ASM ACCOUNTABILITY AND ADMINISTRATIVE REVIEW: 7-0-0
YES: Petrie-Norris, Patterson, Burke, Gray, Lackey, Medina, Rodriguez

ASM APPROPRIATIONS: 15-0-1
YES: Holden, Bigelow, Bryan, Calderon, Luz Rivas, Davies, Fong, Gabriel, McCarty, Levine, Quirk, Robert Rivas, Akilah Weber, Stone, Mullin
ABS, ABST OR NV: Megan Dahle

UPDATED

VERSION: January 24, 2022

CONSULTANT: Landon Klein / P. & C.P. / (916) 319-2200 FN: 0002133