SENATE COMMITTEE ON APPROPRIATIONS
Senator Anthony Portantino, Chair
2021 - 2022 Regular Session

AB 581 (Irwin) - Cybersecurity

Version: June 20, 2022
Urgency: No
Hearing Date: June 27, 2022
Policy Vote: G.O. 14 - 0
Mandate: No
Consultant: Janelle Miyashiro

Bill Summary: AB 581 requires all state agencies to review and implement the National Institute of Standards and Technology (NIST) guidelines, as specified, by July 1, 2023; requires the Office of Information Services (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 guidelines to state agencies and entities by April 1, 2023; and requires the OIS and California Cybersecurity Integration Center (Cal-CSIC) to provide assistance, as specified, upon request by a state agency.

Fiscal Impact: Unknown fiscal impact, in the hundreds of millions of dollars, across all state agencies to review and implement the NIST guidelines (General Fund and various special funds). Costs are variable among state agencies and would depend, among other things, on the entity's size, resource needs, and the extent to which an agency might already be doing this work.

The California Department of Technology (CDT) anticipates:
- One-time cost of approximately $18.0 million and $8.9 million ongoing to implement the program.
- Approximately $123.0 million to provide assistance in implementing the guidelines to other state agencies under CDT's direct authority, which CDT may recover from requesting agencies. Total assistance costs to CDT would vary and depend upon the level of assistance needed or requested.
- Additional unknown, potentially significant costs to provide assistance to state agencies not under CDT's oversight authority, such as the statewide Constitutional Officers, the University of California, and other public agencies.

Background: 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.

Proposed Law:

- Requires all state agencies, as defined, to review and implement the NIST guidelines established pursuant to Section 5 of Public Law 116-207 by July 1, 2023.
    - Authorizes a state agency’s review and implementation of the guidelines to include modifying terms and structures applicable to federal entities to appropriately apply to a state agency.
- Provides that specified agencies and any entity within the executive branch that is under the direct authority of the Governor satisfy the requirement to implement the

guidelines by implementing the standards and procedures published by the chief of OIS.

- 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 entities by April 1, 2023.

- Requires OIS, upon request by any state agency or entity, to provide assistance in implementing the guidelines and standards.

    - Authorizes a state agency to withdraw their request and discontinue any assistance from OIS at any time.

- Requires OIS and the Cal-CSIC, upon request by any state agency or entity, to provide operational and technical assistance on reporting, coordinating, publishing, and receiving information about cybersecurity vulnerabilities of information systems.

    - Authorizes a state agency to withdraw their request and discontinue any operational or technical assistance from the OIS or CCIC at any time.

- Provides that the requirements to implement the guidelines apply to the University of California only to the extent that the Regents of the University of California adopt a resolution to do so.

- States legislative findings and declarations.

Staff Comments: While the total fiscal impact across all state agencies to review and implement the NIST guidelines is unknown, it is likely to be significant. Costs to each state agency will depend on numerous factors, including the size and scope of any potential security vulnerabilities as well as the capacity of each agency to absorb additional information technology (IT) workload within its current resources. For example, various state agencies have reported the following potential fiscal impacts:

- The Business, Consumer Services, and Housing Agency anticipates total costs of approximately $323,000 in the first year, and $315,000 ongoing for an additional IT staff and other hardware and software needs.
- The California Environmental Protection Agency anticipates total costs of approximately $500,000 for two additional IT staff and other operating expenses.
- The Department of Pesticide Regulation anticipates one-time initial costs of approximately $804,000 for additional security tools and equipment, and total ongoing costs of approximately $1.07 million for two additional IT staff and operating supplies and equipment.
- The California Air Resources Board anticipates ongoing costs of approximately $1.29 million for three additional IT staff and operating expenses and equipment.
- The California Department of Corrections and Rehabilitation (CDCR) anticipates total costs of approximately $3.0 million for additional IT staff to implement the program. These costs include both CDCR and California Correctional Health Care Services (CCHCS) resource needs.

- The California Privacy Protection Agency anticipates one-time costs of $455,000 in the first year and $199,000 ongoing for two additional staff to monitor, assess, and implement the guidelines.
- The State Controller's Office anticipates ongoing costs of approximately $400,000 for two additional IT staff to adopt and implement the guidelines and maintain the program.
- The Secretary of State anticipates costs of approximately $1.23 million in the first year and $1.17 million ongoing. Costs include two additional IT staff, testing tools, software, staff time to promulgate regulations, and other ongoing miscellaneous IT resources.
- The California Department of Insurance anticipates costs of $222,000 in Fiscal Year (FY) 2022-23, $1.45 million in FY 2023-24, and $458,000 ongoing to review and implement the guidelines.
- The State Treasurer's Office anticipates one-time implementation costs of approximately $2.15 million and ongoing costs of $1.35 million for additional IT staff to implement the program and conduct trainings, and for other IT operational hardware and software expenses.
- The California Office of Emergency Services and the California Military Department do not anticipate additional fiscal impacts from this bill.

Based on the costs identified above by a small sample of state agencies, statewide costs across all state entities will likely total into the hundreds of millions of dollars.

-- END --