Date of Hearing: May 12, 2021

ASSEMBLY COMMITTEE ON APPROPRIATIONS
Lorena Gonzalez, Chair
AB 581 (Irwin) – As Amended March 25, 2021

Policy Committee:	Privacy and Consumer Protection	Vote: 11 - 0
	Accountability and Administrative Review	7 - 0

Urgency: No State Mandated Local Program: No Reimbursable: No

SUMMARY:

This bill requires, no later than July 1, 2022, all state agencies review and implement guidelines published by the National Institute of Standards and Technology (NIST) for reporting, coordinating, publishing and receiving information about the security vulnerabilities of state information technology (IT) systems. This bill also requires the Office of Information Security (OIS) to review the NIST guidelines established pursuant to the federal Internet of Things (IoT) Cybersecurity Improvement Act, and create, update and publish any appropriate standards or procedures in the State Administrative Manual (SAM) and State Information Management (SIMM) no later than April 1, 2022.

FISCAL EFFECT:

1) Costs (General Fund (GF)) in in the millions of dollars for state agencies to review and implement NIST guidelines on IT security. Specifically, the State Controller's Office (SCO) estimates costs up to $2.2 million dollars annually to the extent SCO's policies are not consistent with NIST guidelines. The California Department of Insurance (CDI) estimates costs of $198,000 in fiscal year (FY) 2021-22, $384,000 in FY 2022-23 and $361,000 annually thereafter to develop, implement and maintain an IT security vulnerability disclosure program. NIST guidelines have not yet been completed and this bill requires guidelines to be implemented by July 1, 2022. Costs, possibly in the millions of dollars across all relevant state agencies, will depend on when NIST guidelines are issued. Public comment on the latest NIST updates closed on February 26, 2021, and final guidelines are expected in June 2021. If NIST issues guidelines this year and this bill becomes effective January 1, 2022, state agencies will have six months to adopt and implement those guidelines. This may create significant workload for state agencies to comply with the requirements of this bill, given the short window of time.

2) Unknown, 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 April 1, 2022 and provide technical assistance to state agencies to comply with the updated regulations. As noted above, costs will depend on when the updated NIST guidelines are issued.

COMMENTS:

1) **Purpose.** According to the author:

> 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.

2) **IoT Improvement Act.** The 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. In December 2020, Congress passed and the President signed into law, the bipartisan IoT Cybersecurity Improvement Act of 2020, which primarily requires NIST to promulgate guidelines relating to the use and management of IoT devices, and the reporting and resolution of security vulnerabilities. Specifically, the IoT Improvement 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 any security vulnerability. This bill parallels the requirements of the IoT 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. NIST issued baseline IoT documents in May 2020 and issued draft regulations for public comment in December 2020. NIST reported concerns from several agencies after submitting documents for public comment that the baseline document and proposed regulations could not be applied to certain technological devices which could result in possibly different standards for different federal agencies. The Insurance Commissioner, the State Treasurer and the State Controller each expressed concern about their ability to comply with the requirements of this bill, given the short timeline and delay of final regulations.

3) **Related Legislation.**

a) AB 809 (Irwin), of the 2021-22 Legislative Session, 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. AB 809 is pending in this committee.

b) AB 1352 (Chau), of the 2021-22 Legislative Session, authorizes the Military Department to perform a security assessment of a local educational agency or school site at the request and expense of the local educational agency. AB 1352 is pending in this committee.

Analysis Prepared by: Kimberly Horiuchi / APPR. / (916) 319-2081