Date of Hearing: April 28, 2021

ASSEMBLY COMMITTEE ON ACCOUNTABILITY AND ADMINISTRATIVE REVIEW
Cottie Petrie-Norris, Chair
AB 581 (Irwin) – As Amended March 25, 2021

SUBJECT: Cybersecurity

SUMMARY: This bill would require state agencies to adopt and implement new National Institute of Standards and Technology (NIST) guidelines on reporting, coordinating, publishing, and receiving information about a security vulnerability relating to information systems. Specifically, **this bill**:

1) Declares that House Resolution 1668, the Internet of Things Cybersecurity Improvement Act of 2020, became law and requires NIST to publish new guidelines on reporting, coordinating, publishing, and receiving information about a security vulnerability relating to information systems by June 2, 2021.

2) Requires all state agencies to review and implement the new NIST guidelines by July 1, 2022.

3) Requires the Chief of the Office of Information Security to review the NIST guidelines and create, update, and publish appropriate standards or procedures in the State Administrative Manual (SAM) and State Information Management Manual (SIMM) by April 1, 2022.

4) Requires a state entity to implement the standards and procedures published in the SAM and SIMM.

5) Requires the Office of Information Security (OIS) to provide assistance in implementing the guidelines when requested by any state agency.

6) Requires the California Cybersecurity Integration Center to provide operational and technical assistance on reporting, coordinating, publishing, and receiving information about cybersecurity vulnerabilities of information systems, when requested by any state agency.

EXISTING LAW:

1) Defines "state agency" as every state office, officer, department, division, bureau, board, and commission. It exempts from the definition of "state agency" the California State University unless explicitly provided.

2) Defines "state entity" as an entity within the executive branch that is under the direct authority of the Governor.

3) Establishes the OIS within the California Department of Technology (CDT) to create, update, and issue information security and privacy policies, standards, and procedures which are included in the SAM and SIMM.

4) Requires state agencies under direct authority of the Governor to adopt and implement policies, standards, and procedures contained in the SAM and SIMM.

5) Authorizes the OIS to conduct or require an ISA of every state agency under direct authority of the Governor.

6) Authorizes the Military Department to perform an ISA on any state agency under the direct authority of the Governor.

FISCAL EFFECT: Unknown

COMMENTS: This bill would require state agencies to review and adopt new NIST guidelines which would potentially improve the ways in which state agencies receive, report, coordinate, and publish security vulnerabilities threatening the state.

According to the author, "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 new 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 new 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 digital infrastructure due to the COVID-19 pandemic, it is now more important than ever to secure our state systems."

House Resolution 1668, the Internet of Things Cybersecurity Improvement Act of 2020 became federal law and requires NIST to publish new guidelines on reporting, coordinating, publishing, and receiving information about a security vulnerability relating to information systems by June 2, 2021. Those guidelines have not yet been published and it is unclear what those guidelines will specifically state. Based on previous NIST guidelines, it is expected that the new NIST guidelines will be reasonable and appropriate for the state to adopt. However, members of the committee may want to consider the appropriateness of requiring state agencies to adopt guidelines that are not yet public. If this bill were to move forward and assuming that the guidelines are made public by June 2, 2021, there will be a limited time to review the new guidelines prior to passage or enactment.

In support, Splunk, Inc. states "with the passage of AB 581, the State of California will add another important tool to its cybersecurity defenses and join leading private sector companies and the U.S. federal government as an important adopter of coordinated vulnerability disclosure (CVD) programs."

With concerns, State Treasurer's Office states "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."

DOUBLE REFERRAL: This bill was previously heard in the Assembly Committee on Privacy and Consumer Protection on April 8, 2021, with a vote of 11-0.

PREVIOUS LEGISLATION:

AB 2564 (Chau) of 2019, which was not referred to a committee and died at the Assembly Desk, was related to this bill.

REGISTERED SUPPORT / OPPOSITION:

Support

Splunk, Inc.

Opposition

None on file

Analysis Prepared by: Jesse Cuevas / A. & A.R. / (916) 319-3600