# SENATE COMMITTEE ON PUBLIC SAFETY

**Senator Aisha Wahab, Chair**
**2023 - 2024 Regular**

| | | | |
|---|---|---|---|
| **Bill No:** | AB 1559 | **Hearing Date:** | July 11, 2023 |
| **Author:** | Jackson | | |
| **Version:** | June 14, 2023 | | |
| **Urgency:** | No | **Fiscal:** | Yes |
| **Consultant:** | MK | | |

**Subject:** ***Elections***

## HISTORY

Source: California Secretary of State

Prior Legislation: None applicable

Support: California Association of Clerks & Election Officials

Opposition: None known

Assembly Floor Vote: 80 - 0

## PURPOSE

***The purpose of this bill is to update existing election record retention, preservation, and destruction requirements to provide clear guidance for electronic voting data, as specified, and to expands and clarifies two existing felonies related to voting technology security.***

*Existing law* defines a "paper cast vote record" to mean an auditable document that corresponds to the selection made on the voter's ballot and lists the contests on the ballot and the voter's selections for those contests. (Elections Code §305.5)

*Existing law* requires, generally, electronic poll books, ballot manufacturers and finishers, BOD systems, voting systems, and RAVBM systems to be approved by the SOS before their use in an election. (Elections Code §§2250, 13004.5, 19201, 19281)

*Existing law* requires a ballot card manufacturer, ballot card finisher, or BOD system vendor to notify the SOS and affected local elections officials in writing within two business days after discovering any flaw or defect that could adversely affect the future casting or tallying of votes. (Elections Code §13004(d))

*Existing law* requires an electronic poll book vendor to notify the SOS and affected local elections officials in writing within 24 hours after discovering any flaw or defect that could adversely affect the future casting or tallying of votes. (2 Code of California Regulations §20161)

*Existing law* requires any magnetic or electronic storage medium, used for a ballot tabulation program or containing election results, to be kept in a secure location, as specified. (Elections Code §15209)

*Existing law* requires specified ballots and identification envelopes to be kept by an elections official unopened and unaltered, as specified, for 22 months following a federal election, and for six months following any other state or local election. (Elections Code §§17301, 17302)

*Existing law* makes it a felony for a person to knowingly, and without authorization, make or have in their possession a key to a voting machine that has been adopted and will be used in elections in California. (Elections Code §18564)

*Existing law* prohibits any part of a voting system from doing any of the following: being connected to the Internet at any time; electronically receiving or transmitting election data through an exterior communication network, including the public telephone system, if the communication originates from or terminates at a polling place, satellite location, or counting center; or, receiving or transmitting wireless communications or wireless data transfers. (Elections Code §19205)

*This bill* defines the term "jurisdiction" to mean any county, city and county, city, or special district that conducts elections pursuant to the Elections Code.

*This bill* authorizes the SOS to impose additional conditions of approval as deemed necessary by the SOS for the certification of electronic poll books, ballot manufacturers and finishers, BOD systems, voting systems, and RAVBM systems.

*This bill* reduces, from two business days to 24 hours, the amount of time that a ballot card manufacturer, ballot card finisher, or BOD system vendor has to notify the SOS and affected local elections officials after discovering any flaw or defect that could adversely affect the future casting or tallying of votes.

*This bill* adds paper cast vote records to the list of election materials required to be kept by a county elections official for 22 months for elections involving a federal office, or 6 months for all other elections.

*This bill* requires any copy of a magnetic or electronic storage medium, used for a ballot tabulation program or containing election results, to be kept in a secure location, as specified.

*This bill* defines the term "ballot printer" to mean any company or jurisdiction that manufactures, finishes, or sells ballot cards, including test ballots, for use in an election conducted pursuant to the Elections Code, and recasts provisions of law that require a ballot printer, as defined, to be approved by the SOS before manufacturing or finishing ballot cards, or accepting or soliciting orders for ballot cards.

*This bill* defines the following terms for the preservation of electronic data related to voting technology:

- "Ballot image" to mean an electronically captured or generated image of a ballot that is created on a voting device or machine, which contains a list of contests on the ballot, may contain the voter selections for those contests, and complies with the ballot layout requirements. A ballot image can be considered a cast vote record.

- "Certified voting technology" to mean any certified voting technologies certified by the SOS, including voting systems, BOD printing systems, electronic poll book systems, or

adjudication systems, and the hardware, firmware, software, proprietary intellectual property they contain, any components, and any products they generate, including ballots, ballot images, reports, logs, cast vote records, or electronic data.

- "Chain of custody" to mean a process used to track the movement and control of an asset through its lifecycle by documenting each person and organization who handles an asset, the date and time it was collected or transferred, and the purpose of the transfer. A break in the chain of custody refers to a period during which control of an asset is uncertain and during which actions taken on the asset are unaccounted for or unconfirmed.

- "Electronic data" to include voting technology software, operating systems, databases, firmware, drivers, and logs.

- "End of lifecycle" to mean the secure clearing or wiping of the certified voting technology so that no software, firmware, or data remains on the equipment and the equipment becomes a nonfunctioning piece of hardware.

- "HASH" to mean a mathematical algorithm used to create a digital fingerprint of a software program, which is used to validate software as identical to the original.

- "Lifecycle" of certified voting technology to mean the entire lifecycle of the certified voting technology from the time of certification and trusted build creation through the end of lifecycle of the certified voting technology.

*This bill* requires the following data to be kept by the elections official, on electronic media, stored and unaltered, for 22 months for those elections where candidates for one or more of the following offices are voted upon: President, Vice President, United States (US) Senator, and US Representative; and for six months for all other state and local elections:

- All voting system electronic data.

- All BOD system electronic data, if applicable.

- All adjudication electronic data.

- All RAVBM system electronic data, if applicable.

- All electronic poll book electronic data, if applicable.

- HASH values taken from the voting technology devices, if applicable.

- All ballot images, if applicable.

*This bill* provides that if a contest is not commenced within the 22-month period or within a six-month period, or if a criminal prosecution involving fraudulent use, using the ballot tally system to mark or falsify ballots, or manipulation of the ballot tally system, is not commenced within the relevant period, the elections official shall have the backups destroyed.

*This bill* authorizes certified voting technology equipment and components that are at the end of lifecycle to be securely disposed of or destroyed with the written approval of the manufacturer and the SOS.

*This bill* requires all of the following to occur for any part or component of certified voting technology for which the chain of custody has been compromised or the security or information has been breached or attempted to be breached:

- The chief elections official of the city, county, or special district and the SOS shall be notified within 24 hours of discovery;

- The equipment shall be removed from service immediately and replaced if possible; and

- The integrity and reliability of the certified voting technology system, components, and accompanying electronic data shall be evaluated to determine whether they can be restored to their original state and reinstated.

*This bill* expands an existing crime that makes it a felony to knowingly, and without authorization, possess a key to a voting machine that has been adopted and will be used in elections in California, to additionally include possessing credentials, passwords, or access keys to such a voting machine.

*This bill* clarifies an existing crime that makes it a felony to interfere or attempt to interfere with the secrecy of voting or ballot tally software program source codes, by adding a provision that states, for the purposes of this paragraph, interferes or attempts to interfere with, includes but is not limited to, knowingly, and without authorization, providing unauthorized access to, or breaking the chain of custody to, certified voting technology during the lifecycle of that certified voting technology, or any finished or unfinished ballot cards.

*This bill* prohibits a voting system from establishing a network connection to any device not directly used and necessary for voting system functions. Prohibits communication by or with any component of the voting system by wireless or modem transmission at any time. Prohibits a component of the voting system, or any device with network connectivity to the voting system, from being connected to the internet, directly or indirectly, at any time.

*This bill* requires a voting system to be used in a configuration of parallel central election management systems separated by an air-gap. Provides that an "air-gap" includes all of the following:

- A permanent central system known to be running unaltered, certified software and firmware that is used solely to define elections and program voting equipment and memory cards.

- A physically-isolated duplicate system, reformatted after every election to guard against the possibility of infection that is used solely to read memory cards containing vote

results, accumulate and tabulate those results, and produce reports.

- A separate computer dedicated solely to this purpose that is used to reformat all memory devices before they are connected to the permanent system again.

*This bill* makes technical, clarifying, and conforming changes

## COMMENTS

### 1. Need for This Bill

According to the author:

> In California, home to nearly 20 percent of the nation's electors, election security is of the highest priority. As the nonpartisan, chief election official for the state, the California Secretary of State's Office works around the clock to ensure every vote is safe and secure.
>
> California has the most stringent voting system testing, certification and use requirements in the country. The Secretary of State has impressively kept our voting security on the cutting edge. For example, Secretary of State's office has administered over $400 million dollars in state and federal funding for voting infrastructure updates, including strengthening the accessibility, accuracy, security, and safety of our elections.

### 2. Expansion of felony for election tampering

Existing law makes it a felony to tamper with, interfere with voting systems, voting software programs etc. before or during an election. This bill clarifies that interferes with or attempts to interfere with to include but not be limited to knowingly, and without authorization, providing unauthorized access to , or breaking the chain of custody to, certified voting technology during the lifecycle of that certified voting technology, or any finished or unfinished ballot cards.

Exiting law also makes it a felony to knowingly and without authorization make or have in his or her possession a key to a voting machine that will e used in elections in this state. This bill updates that definitional to instead prohibit the knowingly and without authorizations the possession of credentials, passwords or access keys to a voting machine that will be used in an election.

### 3. Other changes

This bill passed Senate Elections and Constitutional Amendments on June 20 to look at the other election issues in this bill which include:

- Updating and clarifying existing procedures and requirements to ensure they include electronic election materials, such as paper cast records and magnetic or electronic storage mediums, and establishes specific requirements for the preservation of election data.
- Various provisions that update and expand existing procedures and requirements related to election technology. For example, this bill codifies the authority for the SOS to

impose additional conditions on voting equipment approved for use in any election, and requirements for a vendor to provide notice within 24 hours of any flaw or defect for certain voting equipment. Additionally, this bill clarifies current prohibitions and specifies that a voting system is prohibited from establishing a network connection to any device not directly used and necessary for the voting system functions, and any communication by or with any component of the voting system by wireless or modem transmission.

**4. Argument in Support**

The California Association of Clerks & Election Officials supports this bill stating:

> Existing law requires a ballot card manufacturer, ballot card finisher, or ballot on demand system vendor to notify the Secretary of State and affected local elections officials in writing within 2 business days after discovering any flaw or defect that could negatively impact the future casting or tallying of votes. AB 1559 would require notification within 24 hours. Under current law, voted ballots, are required to be kept by county elections officials for 22 months for elections involving a federal office or 6 months for all other elections. This bill would expand this to include paper cast vote records. The bill would also require county elections officials to keep certain electronic data for 22 months for elections for federal office or six months for all other elections.
>
> Currently, it is a felony punishable by imprisonment for two to four years to knowingly, and without authorization, possess a key to voting equipment that has been adopted and will be used. AB 1559 would expand this crime to include knowing and unauthorized possession of credentials, passwords, or access keys to voting equipment. AB 1559 would also authorize the destruction or secure disposal of certified voting technology at the end of lifecycle with the written approval of the Secretary of State and the manufacturer.
>
> Existing law prohibits a voting system from being connected to the internet and from receiving or transmitting wireless communications or wireless data transfers. This bill would prohibit establishing a network connection to any device not directly used and necessary for voting system functions. The bill would require a voting system to be separated by an air-gap.

**-- END –**