

Date of Hearing: March 29, 2023

ASSEMBLY COMMITTEE ON ELECTIONS
Isaac G. Bryan, Chair
AB 1559 (Jackson) – As Introduced February 17, 2023

SUBJECT: Elections.

SUMMARY: Updates existing election record retention, preservation, and destruction requirements to provide clear guidance for electronic voting data, as specified. Makes it a felony to knowingly, and without authorization, make or possess copies of electronic data related to voting technology, or to provide unauthorized access to certified voting technology, as specified.

Specifically this bill:

- 1) Defines the term “jurisdiction” to mean any county, city and county, city, or special district that conducts elections pursuant to the Elections Code.
- 2) Authorizes the Secretary of State (SOS) to impose additional conditions of approval as deemed necessary by the SOS for the certification of electronic poll books, ballot manufacturers and finishers, ballot on demand (BOD) systems, voting systems, and remote accessible vote by mail (RAVBM) systems.
- 3) 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.
- 4) 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.
- 5) 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.
- 6) 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.
- 7) Defines the following terms for the preservation of electronic data related to voting technology:
 - a) “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.
 - b) “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.

- c) “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.
 - d) “Electronic data” to include voting technology software, operating systems, databases, firmware, drivers, and logs.
 - e) “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.
 - f) “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.
 - g) “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.
- 8) 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:
- a) All voting system electronic data.
 - b) All BOD system electronic data, if applicable.
 - c) All adjudication electronic data.
 - d) All RAVBM system electronic data, if applicable.
 - e) All electronic poll book electronic data, if applicable.
 - f) HASH values taken from the voting technology devices, if applicable.
 - g) All ballot images.

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.

- 9) 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.
- 10) 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:
 - a) The chief elections official of the city, county, or special district and the SOS shall be notified within 24 hours of discovery;
 - b) The equipment shall be removed from service immediately and replaced if possible; and,
 - c) 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.
- 11) 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.
- 12) Makes it a felony to knowingly, and without authorization, make or possess copies of electronic data, and to knowingly, and without authorization, provide unauthorized access to, or to break the chain of custody to, certified voting technology during the lifecycle of that technology, or any finished or unfinished ballot cards, as specified.
- 13) 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.
- 14) 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) 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.
 - b) 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.
 - c) 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.
- 15) Makes technical, clarifying, and conforming changes.

EXISTING LAW:

- 1) 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)
- 2) 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)
- 3) 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))
- 4) 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)
- 5) 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)
- 6) 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)
- 7) 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)
- 8) 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)

FISCAL EFFECT: Unknown. State-mandated local program; contains a crimes and infractions disclaimer.

COMMENTS:

- 1) **Purpose of the 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 that includes:

- Any new voting system in California must receive certification and undergo months of testing, including 1) functional testing, 2) source code review, 3) red team security penetration testing that involves open-ended vulnerability testing of the voting system, and 4) accessibility and volume testing.
- Voting systems cannot connect to the internet.
- All voting systems are air-gapped and kept separate from all other systems.
- Every ballot must either be paper or have a voter-verifiable paper audit trail.
- Prior to every election a logic and accuracy test must be conducted to verify the functioning of the voting system.
- Following every election, the elections officials must conduct a manual audit of a random 1% of ballots to ensure vote count machines are accurate.

The Secretary of State's Office of Voting System Technology and Assessment (OVSTA) requires that voting systems once certified for use in California has strict chain of custody.

The 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.

Even with all that California has done – and spends – we must continue to do more to ensure that our requirements for chain of custody, retention, use, and security are clear and unambiguous.

Now California must act to ensure that voting systems and associated material is protected from those who would act irresponsibly in their privileged role that grants them access to this highly sensitive material. We must also send a strong message that these privileged individuals will suffer substantial consequences for attempting to undermine voters and one of the most basic principles of our democracy – fair and secure elections.

- 2) **Voting Technology:** The Legislature has approved various bills to ensure California has the most rigorous and stringent voting system and voting equipment standards and approval procedures. Notably, SB 360 (Padilla), Chapter 602, Statutes of 2013, made significant changes to procedures and criteria for the certification and approval of a voting system, required the SOS to adopt and publish voting system standards and regulations governing the use of voting systems, and required those standards to meet or exceed federal voluntary voting system guidelines (VVSG) set forth by the US Election Assistance Commission (EAC) or its successor agency, as specified.

Accordingly, in 2014, California established its own standards – California voting system standards (CVSS) – for electronic components of voting systems which were derived from

the EAC's VVSG versions 1.1 and 2.0. The CVSS provides a set of specifications and requirements to which voting systems are required to be tested to determine if they provide all the basic functionality, accessibility, and security capabilities required of voting systems. All voting technology, including, but not limited to voting systems, electronic pollbooks, and RAVBM systems, are required to be certified for use prior to being sold or used in any California election.

In counties that use electronic voting systems, state law requires election officials to provide paper ballots at the polling place. State law additionally prohibits any part of a voting system from being connected to the Internet at any time, and California's voting system standards prohibit voting systems from having the capability to communicate individual votes or vote totals over public communications networks or from having wireless communications capabilities.

This bill includes 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.

- 3) **Electronic Election Materials:** Existing law specifies the requirements for retention, preservation, and destruction of certain election materials, such as ballots, voter rosters and indexes. However, according to the author and sponsor of this bill, existing law related to the storage, maintenance, preservation and destruction of election data has not kept pace with the evolution of voting technologies and does not provide clear guidance for retention of electronic voting data. Accordingly, this bill updates and clarifies 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.
- 4) **New Threats to Election Integrity:** According to news articles, since the 2020 general election, there have been suspected or attempted "insider" security breaches in local election offices across the nation. One highly publicized breach occurred in Colorado in which a county clerk was indicted for her role in facilitating unauthorized access to voting machines.

According to the author and sponsor, while there have not been any suspected or attempted security breach incidents in California, this bill will nonetheless strengthen existing law and provide clear authority to prosecute should a violation occur. Specifically, this bill expands existing law to make it a felony to knowingly, and without authorization, possess credentials, passwords, or access keys to a voting machine that has been adopted and will be used in elections in California. Additionally, this bill makes it a felony to knowingly, and without authorization, make or possess copies of electronic data, to provide unauthorized access to, or to break the chain of custody to, certified voting technology during the lifecycle of that technology.

- 5) **Critical Infrastructure Designation:** On January 6, 2017, then-Secretary of the federal Department of Homeland Security (DHS) Jeh Johnson announced that he was designating election infrastructure in the country as critical infrastructure, a decision that was later reaffirmed by the Trump administration. According to information from DHS, critical infrastructure is a designation "established by the Patriot Act and given to 'systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.'" In his announcement, Secretary Johnson noted that the designation generally gives DHS the ability to provide additional cybersecurity assistance to state and local elections officials, but does not mean that there will be new or additional federal regulation or oversight of the conduct of elections by state and local governments.

The DHS has prepared a Cybersecurity Services Catalog for Election Infrastructure that outlines the services and other assistance available to the election infrastructure community, including state and local elections officials. Among the services provided are various no-cost cybersecurity assessments, information sharing about cybersecurity threats, cybersecurity training, assistance in cyber incident planning and cyber incident response, and network protection.

- 6) **Technical Amendments:** After the committee's deadline for pre-committee author's amendments, the author proposed technical amendments to clarify the definition of the term "chain of custody." Committee staff recommends the following technical amendments:

On page 9, starting in line 6, amend the bill as follows:

(c) "Chain of custody" means a process used to track the movement and control of a certified voting technology, pursuant to subsection (b) of section 17600, ~~an asset~~ through its lifecycle by documenting each person and organization who handles a certified voting technology ~~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 the certified voting technology ~~an asset~~ is uncertain and during which actions taken on the certified voting technology ~~asset~~ are unaccounted for or unconfirmed.

- 7) **Double Referral:** This bill is double referred to the Assembly Public Safety Committee.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file.

Opposition

None on file.

Analysis Prepared by: Nichole Becker / ELECTIONS / (916) 319-2094