Date of Hearing: April 25, 2023
Counsel: Liah Burnley

ASSEMBLY COMMITTEE ON PUBLIC SAFETY
Reginald Byron Jones-Sawyer, Sr., Chair

AB 1559 (Jackson) – As Amended April 5, 2023

As Proposed to Be Amended In Committee

SUMMARY: Clarifies that it is a criminal offense to interfere with voting by knowingly providing unauthorized access to certified voting technology. Specifically, **this bill**:

1) Updates existing election record retention, preservation, and destruction requirements to provide clear guidance for electronic voting data, as specified.[1]

2) Clarifies that it is a felony to knowingly provide unauthorized access to, or break the chain of custody to, certified voting technology during the lifecycle of that technology, or any finished or unfinished ballot cards.

3) Defines "chain of custody" as a process used to track the movement and control of certified voting technology, through its lifecycle by documenting each person and organization who handles certified voting technology, the date and time it was collected or transferred, and the purpose of the transfer.

4) Defines a "break in the chain of custody" as a period during which control of the certified voting technology is uncertain and during which actions taken on the certified voting technology are unaccounted for or unconfirmed.

5) Defines "certified voting technology" as any certified voting technologies certified by the Secretary of State, including voting systems, ballot on demand 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.

6) Defines "lifecycle" of certified voting technology as 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.

EXISTING LAW:

1) Provides that it is a felony, punishable by imprisonment for two, three, or four years to, before or during an election, tamper with, interfere with, or attempt to interfere with, the correct operation of, or willfully damage in order to prevent the use of, any voting machine,

[1]This bill has been double referred to the Assembly Elections Committee. Accordingly, the primary focus of this analysis is the penalty provisions that fall within the jurisdiction of this Committee.

voting device, voting system, vote tabulating device, or ballot tally software program source codes. (Elec. Code, § 18564, subd. (a).)

2) Provides that it is a felony, punishable by imprisonment for two, three, or four years to, before or during an election, interfere or attempt to interfere with the secrecy of voting or ballot tally software program source codes. (Elec. Code, § 18564, subd. (b).)

3) Provides that it is a felony, punishable by imprisonment for two, three, or four years to, before or during an election, knowingly, and without authorization, possess a key to a voting machine that will be used in elections in this State. (Elec. Code, § 18564, subd. (c).)

4) Provides that it is a felony, punishable by imprisonment for two, three, or four years to, before or during an election to willfully substitute or attempt to substitute forged or counterfeit ballot tally software program source codes. (Elec. Code, § 18564, subd. (d).)

5) Provides aiding and abetting in the commission of any of the above offenses is punishable by imprisonment in the county jail for a period of six months or in the state prison for 16 months or two or three years. (Elec. Code, § 18565.)

6) Prohibits knowingly accessing and without permission altering, damaging, deleting, destroying, or otherwise using any data, computer, computer system, or computer network in order to wrongfully control or obtain property or data. This offense is punishable as a felony by imprisonment for 16 months, or two or three years and a fine not exceeding $10,000, or as a misdemeanor, by imprisonment in a county jail not exceeding one year, by a fine not exceeding $5,000, or by both. (Pen. Code, § 502, subds. (c)(1) & (d)(1).)

7) Prohibits knowingly accessing and without permission taking, copying, or making use of any data from a computer, computer system, or computer network, or any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network. This offense is a felony, punishable by imprisonment pursuant for 16 months, or two or three years and a fine not exceeding $10,000, or a misdemeanor, punishable by imprisonment in a county jail not exceeding one year, by a fine not exceeding $5,000, or by both. (Pen. Code, § 502, subds. (c)(2) & (d)(1).)

8) Requires the court to consider prohibitions on access to and use of computers in determining the terms and conditions applicable to a person convicted of any of the above offenses. (Pen. Code, § 502, subd. (k).)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Author's Statement**: 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.

- 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."

9) **Need for this Bill**: This bill would clarify that it is a felony to knowingly provide unauthorized access to, or break the chain of custody to, certified voting technology during the lifecycle of that technology, or any finished or unfinished ballot cards.
Elections Code section 18564 makes corruption of voting a felony, punishable by imprisonment for two, three, or four years. (Elec. Code, § 18564.) This statute generally prohibits tampering, interfering with, prohibiting the use of voting systems and ballot or tally software program source codes; interfering with the secrecy of voting; the unauthorized possession of a key to a voting machine; and, substitution or forged or counterfeit ballot tally software program source codes. (*Ibid*.) This bill clarifies that a person who provides unauthorized access to voting technology or unfinished ballot cards interferes with the use of voting systems. This clarification is necessary given updates to election technology certified

for use in California.

This conduct can also be prosecuted as a misdemeanor or felony under the State's hacking statute, Penal Code section 502. Under this law, a person is guilty of an offense if they knowingly access, without permission, any data, computer, computer system, or computer network in order to wrongfully control or obtain property or data. This would include voting systems. If convicted for a felony, the offense is punishable by imprisonment for 16 months, or two or three years and a fine not exceeding $10,000, or as a misdemeanor, by imprisonment in a county jail not exceeding one year, by a fine not exceeding $5,000, or by both. (Pen. Code, § 502, subds. (c)(1) & (d)(1).) In addition to fines and imprisonment, a court can also order forfeiture of any computer system used by the person to commit the offense and prohibit the person from accessing and using computers. (Pen. Code, § 502, subd. (k).) In addition, existing law authorizes the Secretary of State (SOS), and in some cases the Attorney General (AG) and county elections officials, to take civil legal action regarding the security of voting systems and the conduct of elections. The penalty is not to exceed $50,000 for each act and for injunctive relief. (Elec. Code, § 18564.5.)

2) **Argument in Support**: According to the *California Secretary of State* (SOS), "AB 1559 provides that the storage, maintenance, and destruction of election material are clear in law by updating the preservation guidelines of election materials, covering the lifecycle of voting technology. Specifically, this measure defines the parameters of the chain of custody of voting technology not yet covered in existing law."

3) **Related Legislation**: AB 1593 (Berman) would make it a misdemeanor for any person to vote or to attempt to vote both in an election held in this state and in an election held in another state on the same date. AB 1593 is pending in the Assembly Appropriations Committee.

4) **Prior Legislation**:

   a) AB 777 (Harper), of the 2017-2018 Legislative Session, would have increased the maximum fine amount from $1,000 to $10,000 for fraudulently signing a ballot.

   b) SB 1376 (Perata), Chapter 813, Statutes of 2004, authorized the SOS, and in some cases the AG and county elections officials, to take legal actions regarding the security of voting systems and the conduct of elections.

REGISTERED SUPPORT / OPPOSITION:

Support

California Secretary of State (Sponsor)
California Association of Clerks & Election Officials

Opposition

None submitted.

Analysis Prepared by: Liah Burnley / PUB. S. / (916) 319-3744