Shirley N. Weber, Ph.D.
California Secretary of State
Office of Voting Systems Technology Assessment
1500 11th Street, 6th Floor | Sacramento, CA 95814 | 916.695.1680 | votingsystems@sos.ca.gov

October 18, 2024

County Clerk/Registrar of Voters (CC/ROV) Memorandum #24220

TO: All County Clerks/Registrars of Voters

FROM: /s/ Rodney Rodriguez
Office of Voting Systems Technology Assessment

RE: OVSTA: Senate Bill 1328 Overview

Senate Bill (SB) 1328 (Chapter 1328, Statutes of 2024) was signed by Governor Gavin Newsom on September 25, 2024, and went into immediate effect. The bill authorizes the Secretary of State (SOS) to impose additional conditions of approval for electronic poll books, ballot manufacturers and finishers, ballot on demand (BOD) systems, voting systems, and remote accessible vote by mail (RAVBM) systems.

Moreover, SB 1328 updates existing election record retention, preservation, and destruction requirements to provide clear guidance for electronic voting data. Additionally, it expands and clarifies an existing felony related to voting technology security.

The added and amended statutes are summarized and explained in the following sections.

Changes Affecting Retention

1) Adds that a copy of a magnetic or electronic storage medium, used for the ballot tabulation program or containing election results, in addition to the original mediums, also shall be kept in a secure location and also shall be retained for either six months (local election) or 22 months (federal election), from the date of the respective election, or so long thereafter as any contest involving the vote at the election remains undetermined. (Elec. Code, § 15209.)

   Please note that counties may continue to use/reuse their voting technology-specific election storage media, such as hard drives and removable media, provided an unaltered copy of relevant election material is preserved.

2) Adds paper cast vote records (typically the output of an RAVBM system and defined in Sections 305.5 and 19271 as "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") 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 six months for all other elections. (Elec. Code, §§ 17301(b)(2), 17302(b)(2).)

   Also adds voted conditional voter registration ballots and conditional voter registration voter identification envelopes to that list of election materials required to be kept by a county elections official for 22 months for elections involving a federal office, or six months for all other elections. (Elec. Code, §§ 17301(b)(6), (7), 17302(b) (6), (7).)

3) Defines "ballot image" as 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. (Elec. Code, § 17600(a).)

   The Secretary of State is of the opinion that while a ballot image can be viewed by an observer during the post-election audit or recount processes, copies shall not be provided to a requestor nor posted on the internet. (See, Cal. Code Regs., tit.2, § 20357(b).)

4) Defines "electronic data" to include "voting technology software, operating systems, databases, firmware, drivers, and logs." (Elec. Code, § 17600(d).)

   Cast vote record data reports are electronic data. It is the opinion of the Secretary of State that these reports may be provided to requesters under the following specific conditions to ensure compliance and protect voter privacy and the secrecy of a voter's ballot:

   a) Reports should be delivered in a secure, locked PDF format.
   b) For precincts with ten or fewer voters the data should be redacted to safeguard voter privacy.
   c) The frequency of report release is at the discretion of the jurisdiction, provided it does not interfere with the administration of elections.

   Please note that the following data is not public information and is protected by privileges and exemptions and shall not be released:

   a) Voting technology software.
   b) Operating systems.
   c) Databases.
   d) Firmware drivers.
   e) Logs.

   (See, Gov. Code, §§ 7922.000, 7927.705, 7929.210 and 7930.205; Elec. Code, §§ 17600(b), 19214.)

5) Defines "HASH" as "a mathematical algorithm used to create a digital fingerprint of a software program, which is used to validate software as identical to the original." (Elec. Code, § 17600(f).)

6) Adds a list of the data (set forth below) that shall be kept by the elections official, on electronic media, stored and unaltered, for 22 months (federal election) or six months (state or local election) from the date of the respective election:

   a) All voting system electronic data.
   b) All ballot on demand system electronic data, if applicable.
   c) All adjudication electronic data.
   d) All remote accessible vote by mail 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, if applicable.

   (Elec. Code, §§ 17601(a), (b), 17602(a), (b).)

7) Adds that if an election contest is not commenced within the 22-month period (federal election) or within a six-month period (state or local election), 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 above-mentioned time periods, the elections official shall have the backups destroyed. (Elec. Code, §§ 17601(c), 17602(c).)

Changes Affecting Voting Technology Vendors and Voting Systems

1) Defines "jurisdiction" as "any county, city and county, city, or special district that conducts elections pursuant to this code." (Elec. Code, § 327.5.)

2) 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, ballot on demand (BOD) systems, voting systems, and RAVBM systems before their use in an election. (Elec. Code, §§ 2550(d), 13004(b), 13004.5(a), 19201(a), 19281(a).)

3) Reduces, from two business days to 24 hours, the amount of time that a ballot card manufacturer or ballot card finisher, must 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. (Elec. Code, § 13004(d).)

   Also adds the same 24-hour notification requirement to BOD system vendors. (Elec. Code, § 13004.5(d).)

4) Defines "lifecycle" and "end of lifecycle". (Elec. Code, § 17600(e), (g).)

Adds that certified voting technology equipment and components that are at the end of lifecycle may be securely disposed of or destroyed with the written approval of the manufacturer and the SOS. (Elec. Code, § 17603(a).)

5) 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. (Elec. Code, § 19205(c)(2).)

6) Defines "air-gap" for purposes of subdivision (d) of Section 19205. (Elec. Code, § 19205(d)(2).)

   Requires a voting system to be used in a configuration of parallel central election management systems separated by an air-gap, as specified. (Elec. Code, § 19205(d)(1).)

Guidance for Security Breaches, Compromises, Crimes

1) Defines "certified voting technology" and "chain of custody". (Elec. Code, § 17600(b), (c).)

   Requires all 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 be notified within 24 hours of discovery.
   b) The equipment be removed from service immediately and replaced if possible.
   c) The integrity and reliability of the certified voting technology system, components, and accompanying electronic data be evaluated to determine whether they can be restored to their original state and reinstated.

   (Elec. Code, § 17603(b).)

2) 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 defines "interfering or attempting to interfere with", to include 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. (Elec. Code, § 18564(a)(2).)

3) Expands an existing crime such that it is now 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. (Elec. Code, § 18564(a)(3).)

If you have any questions, please contact the Office of Voting Systems Technology Assessment at votingsystems@sos.ca.gov.