

**Secretary of State**  
**Recommended Guidelines**  
**June 20, 2007**

**Permitted Use of Electronic Roster Systems**

The Secretary of State's office has been contacted by voting system vendors and several counties who are interested in deploying electronic roster systems in California.

State law requires the Secretary of State to approve all voting systems before they can be sold in California or used in a California election. [Elections Code §19201(a)] The California statutory definition of a "voting system" was written in 1976 and defines a "voting system" as "any mechanical, electromechanical, or electronic system and its software, or any combination of these used to cast or tabulate votes, or both." [Elections Code §362]. The California statutory definition of "software" includes "all programs, voting devices, cards, ballot cards or papers, operating manuals or instructions, test procedures, printouts, and other nonmechanical or nonelectrical items necessary to the operation of a voting system." [Elections Code §355].

Electronic roster systems have the potential to offer increased efficiencies in election administration that benefit voters and county elections officials. To the degree an electronic roster system may store the entire list of registered voters in a jurisdiction, it may prevent voter disenfranchisement by allowing a registered voter who appears at the wrong polling place to be redirected to the correct polling place, allowing them to vote the correct ballot.

However, as with many electronic systems in use today, an electronic roster system is not without its risks. As the "gatekeeper" to voting, an electronic roster system determines a voter's eligibility to cast a ballot and which ballot style should be provided to a voter. As automated electronic implementations of the traditional paper roster, an electronic roster is subject to the same types of concerns that have been raised about electronic voting systems in recent years. The failure of an electronic roster system could lead to a significant disenfranchisement of voters, whether through programming bugs, malicious attacks or human error in the setup, deployment and operation of such a system. If an electronic roster system contains confidential voter data, such as voter identification numbers, addresses, telephone numbers and electronic mail addresses of registered voters within a county, the theft or compromise of such an electronic roster system poses a grave security risk to those voters.

Electronic roster systems vary tremendously in their functions and features. The degree to which an electronic roster system interacts with a certified voting system dictates whether an electronic roster system itself needs to be federally certified and state certified as part of a voting system before it can be used in California.

The Secretary of State has determined that in cases where an electronic roster system does not interface electronically with any part of a voting system, the electronic roster system does not fall under the current California statutory definition of a "voting system." Therefore, a jurisdiction may use an electronic roster system without state certification, but solely in these limited circumstances.

Jurisdictions reviewing the cost of an electronic roster system may be counting on the future use of all of the utilities offered by the system – including those functions that require the electronic roster system to interact electronically with a certified voting system – in order to fully amortize the cost of that electronic roster system. The Secretary of State cautions jurisdictions that in these cases, an electronic roster system will be required to be certified as a “voting system” under Elections Code §362 before the full value of those benefits can be realized.

Examples of interfaces that would make an electronic roster system part of a voting system include, but are not limited to:

- Using an electronic roster system to burn smart cards or otherwise interact electronically with the voting equipment in a polling place to activate voting devices for voting, or to communicate the assigned ballot style for a voter;
- Using an electronic roster system to calculate and provide voter participation statistics to the vote tabulation system for purposes of calculating turnout; and
- Using an electronic roster system to assign and track provisional ballots or provisional ballot identification numbers.

In these cases, an electronic roster system would be functioning as part of a voting system, and thus would be required to be certified before it could be used in California.

The Secretary of State urges jurisdictions that are considering the use of an electronic roster system to consider adopting the following best practices:

- **Contingency Planning** – Jurisdictions should have a backup plan in place to ensure that voters will not be affected or inconvenienced should the electronic roster system fail or malfunction on Election Day. Jurisdictions should have a contingency plan on file with the Secretary of State’s office to ensure, for example, that if the electronic roster system fails some time during the election, poll workers will know who is eligible to vote and what the appropriate ballot style is for that voter, as well as what process will be in place to determine who has and has not voted.
- **Training** – Jurisdictions should adopt a formal training program to ensure that poll workers receive appropriate training and are comfortable using the electronic roster system technology on Election Day.
- **Security** – Jurisdictions should be familiar with what, if any, safeguards are built into the electronic roster system and equipment to prevent or detect tampering or alteration of the data during storage, during transport to and from the polling place, and throughout Election Day. Jurisdictions should establish and enforce publicly-disclosed written chain-of-custody controls to prevent and detect tampering over the life and use of an electronic roster system.
- **Testing** – Jurisdictions should establish and enforce publicly-disclosed testing processes and procedures for pre-election and post-election testing of the electronic roster system.

- **Protection of Voter Data** – Jurisdictions should establish and enforce a plan to ensure that confidential data about voters stored on the electronic roster system and on any components located in the polling place is protected from unauthorized access, such as if an electronic roster system device is stolen.