



# NEWS RELEASE

CALIFORNIA SECRETARY OF STATE **KEVIN SHELLEY**

KS04:011

FOR IMMEDIATE RELEASE  
Thursday, February 5, 2004

Contact: Doug Stone  
916-653-6575

## **Secretary of State Kevin Shelley Issues Security Directive on Electronic Voting**

*Shelley Directs Counties to Put Security Measures in Place for March Primary*

SACRAMENTO, CA – California Secretary of State Kevin Shelley today ordered county elections officials to implement additional security measures for the March 2, 2004 primary to protect voters against problems that could arise from the use of new computerized voting machines.

Last year, Shelley directed that all electronic voting systems certified for use in California produce an accessible voter verified paper trail so voters can check the accuracy of the machines and verify that their vote has been recorded properly. While the technology to accomplish this is presently being developed, Shelley's interim measures are intended to address some of the concerns raised in recent studies, which have pointed to security issues with touchscreen systems.

"The right to vote is the cornerstone of our American democracy. Voters must have confidence that their vote will be counted as it is cast," said Shelley.

"New technologies create new challenges, and our highest priority is to meet those challenges so that voting machines are accurate and secure," Shelley said. "These security enhancements provide our voters additional confidence that votes cast during the March 2 election will be accurately counted."

In addition to requiring these additional measures, Shelley also called for Diebold, a manufacturer of touchscreen systems used in California counties, to provide his office with the "source code" of software being used in the Diebold systems. The source code will be reviewed by independent experts selected by the Secretary of State.

In 2003, Diebold, without authorization, installed untested software on machines in at least four counties. The Secretary of State's investigation into Diebold's conduct is ongoing. Shelley has demanded that Diebold provide documents related to the investigation no later than February 15, 2004.

"Election vendors should be much more aggressive in providing security measures than they have been up to now. Since they haven't, I am directing the counties to implement the following that are designed to prevent tampering with electronic voting systems."

-more-

These measures include:

- State testing of randomly selected voting machines in every county on election day. These tests, called “parallel monitoring,” will be designed, conducted and recorded by independent experts. California is the first state to implement this requirement, which has been recommended by voting security experts;
- Requiring that counties retain images of each ballot cast, not merely vote totals;
- Posting the results of voting on each voting machine at each precinct for public viewing at the conclusion of voting;
- Prohibiting the use of any wireless devices, including cellular telephones, in connection with electronic voting;
- Requiring that electronic voting machines operate as “stand alone” systems at all times, not connected to the internet;
- Requiring additional security measures when telephone lines are used to report vote totals at the conclusion of voting; and
- Requiring that each county and each voting machine manufacturer prepare a voting equipment security plan, to be reviewed by state officials.