SECRETARY OF STATE
KEVIN SHELLEY
STATE OF CALIFORNIA

February 5, 2004

TO: All County Clerks/Registrars of Voters (04043)

FROM: _____
KEVIN SHELLEY
Secretary of State

SUBJECT: **SECURITY MEASURES FOR TOUCH SCREEN (DRE) VOTING SYSTEMS FOR THE MARCH ELECTION**

There has been substantial public concern expressed about the security of DRE voting systems. These concerns are underscored by a recent study released by the state of Maryland citing ongoing security concerns regarding DRE systems.

As election officials, we have a responsibility to take proactive steps to assure voters that their votes will be counted as cast. As you know, I recently directed that all DRE voting system in use in California must include an "Accessible Voter Verified Paper Audit Trail" (AVVPAT). This technology is not available for the March 2, 2004 election. In light of the recent studies, we must address the public's concern on this issue for this election. Accordingly, listed below are several security measures for DRE machines for the March 2, 2004 Primary election. These measures are being required pursuant to Government Code section 12172.5,

Elections Code sections 13002, 15001 et seq., 19370, and the procedures adopted for use of voting equipment in California.

As an additional security precaution, with respect to the ongoing investigation of Diebold, I have directed that the source code for the TSx system be provided to my office prior to the March election.

1. PARALLEL MONITORING

One significant concern that has been raised is the possibility that unauthorized programmers could illegally manipulate the software that counts ballots on DRE equipment. My office will be implementing a program to randomly select voting machines to be set aside for experts to vote on March 2, 2004. These machines will be voted exactly as if they were in polling places, any anomalies will be detected, and appropriate remedies will be pursued. I will provide more details on the procedures for this program in the accompanying CCROV.

2. PROHIBIT THE USE OF NETWORK CONNECTIONS AND WIRELESS TECHNOLOGY

To ensure the integrity of the voting process, and to prevent "hackers" from gaining access to voting equipment, no voting equipment used at the March 2, 2004 election shall be permitted to be connected during voting hours to any exterior network and no connection to the Internet shall be permitted at any time. In addition, modem access to GEMS must be enabled only when uploads are expected. Finally, no voting equipment will be permitted to include the hardware necessary to permit wireless transmission, and no communication of votes or vote totals will be permitted to be transmitted using wireless technology.

3. POST RESULTS AT EACH POLLING PLACE

Some members of the public and the media have indicated concern that once the results of the vote leave the polling place citizens have no ability to check on whether the results from that polling place are accurately conveyed to the central counting facility. Therefore, a copy of the results from each voting unit that is capable of printing out a tabulation of the results shall be posted for public inspection for at least 24 hours outside each polling place.

4. RECORD OF THE VOTE

As part of the official canvass for the March 2, 2004 election, a complete copy of the images of the voted ballots cast on each touch screen (DRE) voting machine used in the election shall be printed out on paper for each precinct that is subject to the one percent manual recount or other official recount or contest. The paper record shall be used for the one percent manual recount to audit the machine-tabulated total unless there is evidence that the paper record has been corrupted or is incomplete.

For official recounts other than the one percent manual recount or for contests, tinted and watermarked paper or paper overprinted with a design shall be used. The paper version of the images shall be utilized for purposes of any such recount or contest unless there is evidence that the paper record has been corrupted or is incomplete.

In addition, as part of the semi-official canvass for the March 2, 2004 election, counties utilizing touch screen (DRE) voting systems shall produce at least four original CD-ROMs or DVD-ROMs containing images of the voted ballots cast on each touch screen (DRE) voting machine used in the election. Two of the CD-ROMs or DVD-ROMs shall immediately be filed with the Secretary of State. Two of the CD-ROMs or DVD-ROMs shall be retained by the county elections official.

5. ELECTION MONITORS

The issue of voter confidence in the voting systems is critical. In order to assure the public that someone is watching the process for the primary election on March 2, 2004, and that efforts to manipulate the voting process will be prevented or detected, my office will provide Election Monitors in each of the jurisdictions using DRE equipment in the March election. These Monitors will travel from polling place to polling place and report immediately any instances of equipment malfunction or attempts to tamper with voting equipment. Similarly, Monitors will be on-site for the counting of the ballots at the central counting facility. These Monitors shall be provided Secretary of State identification, and shall be granted unrestricted access to polling places.

6. ADDITIONAL MEASURES

In addition to the important security measures outlined above, there are a number of procedural steps that must be taken for the March 2, 2004 election to provide public confidence in the voting process. These include:

A. Each county must prepare and submit to the Secretary of State by February 20, 2004, an "Election Security Plan" that addresses both the physical security of the voting equipment, software, and firmware and the internal security controls (e.g. software access controls, hardware access controls, password management, etc.) for the voting system. Each plan will be independently reviewed.

B. Similarly, each vendor of DRE equipment used in the March election must submit to the Secretary of State by February 17, 2004, an "Election Security Plan" that completely describes the technical and physical securities of voting and vote counting equipment, software, and firmware. Each plan will be independently reviewed.

C. Each county shall prepare and submit to the Secretary of State by February 17, 2004, an "Election Observer Panel Plan" (EOPP) that specifies the procedures for public participation in and observation of the election process, including the Logic And Accuracy testing for voting equipment and vote counting equipment. The EOPP will also include publicizing the opportunity and procedure for public observation.

D. If the Logic and Accuracy testing is conducted using an automated vote script, the testing shall also include a randomized and statistically significant manual entry of votes as a check against the automated script. All test scripts, automated and manual, shall be retained until the period for contesting the election has expired.

E. Each county shall provide a copy of their tabulation software for escrow with the Secretary of State by February 25, 2004. This software must be able to duplicate the county tabulation of election results.

F. Each county shall notify the Secretary of State by February 17, 2004, of the membership of the Logic and Accuracy Board and to send to the Secretary of State a copy of the certificate of that board attesting to the results of pre-election testing of the voting and vote counting equipment. The county shall permit and encourage public participation, as appropriate, on the Logic and Accuracy Board.

G. As specified in the procedures adopted for use of voting equipment in California, and to prevent undetected tampering, serialized or other secure tamper-proof devices/seals must be placed on all ports where memory cards are inserted. Poll workers must log any instance of suspected tampering and no machine shall be used if tampering is evident. An audit log of any action or operation on any voting equipment or software shall be maintained and retained until the period for contesting the election has expired.

H. For those DRE systems that use a "voter card" or "smart card" to activate voting, the card shall not be issued to a voter until a voting station is available. If lines are to form, ensure that they form at the registration table and not at the voting stations.

I. County "troubleshooters", "rovers" or other election deputies circulating to polling places on election day should survey each polling site for any evidence of tampering or attempted intrusion into the voting equipment and immediately report to Secretary of State Monitor.

J. For those counties using DRE equipment, during transportation of election materials to the central count or remote count locations, all election media must be in the possession of at least two election officials/poll workers.

K. The election official shall ensure the protection of the election tabulation process by securing the premises where the vote tabulation is being conducted and not allowing unauthorized and unescorted personnel to be in contact with tabulation equipment.

L. After tabulation, printed results tapes and a backup copy of the tabulation shall be placed in locked storage in a secure location, and shall remain there until the expiration of the period for challenging elections and for as long as required by law, unless a court orders their release.

M. On Election night during tabulation, or following tabulation, all of the event logs, ballot images and summary totals from each cartridge used in the election shall be backed up to the tabulation database.

B&e/security15-024