MAJOR ISSUES AND QUESTIONS ADDRESSED BY THE TASK FORCE

1. COMPUTER SECURITY

One question the Task Force addressed was: Is there evidence of a security issue with DRE voting systems and, if so, what is the nature and probability of the security issue?

The essential argument espoused by several computer scientists is that computerized voting equipment requires reliance on a “black box” and that it is possible that subtle program flaws can affect vote recording or “malicious code” can be added to software in that voting equipment in a way that is extremely difficult to detect. By way of example, this malicious code could be added by a “rogue programmer” and be timed to activate at a future election date to switch 1% of the votes across many jurisdictions for candidates of party A to the candidate of party B. Theoretically, malicious code could also be inserted by a voting system vendor conspiring to alter an election or by others.

The Task Force agrees that, in theory, there is a possibility of a security threat with DRE voting equipment. The Task Force, however, disagrees about the likelihood of the possibility that malicious code could be added to a voting system and be undetected by the federal, state, and local independent testing authorities. Some members (including the computer scientists on the Task Force) assert a high risk while others assert a very low probability.

But the Task Force agrees that there is no proven instance of such an attempt at fraud that has happened in the number of years that DRE voting equipment has been in use.

The Task Force further agrees that setting aside a number of touch screen voting systems on election day, equipment that was prepared exactly like all other equipment used by voters but which is instead voted by trained personnel, can increase the likelihood of detection of attempts by “rogue programmers” or others to manipulate the software of a voting system. This Election Day sampling would be conducted under precise conditions to exactly replicate those at the polling place.

As the computer industry has evolved, there has been a corresponding evolution of “hackers” and others to disrupt or defraud computer systems. In response to this, there has also been the development of an industry to provide security to computer systems. This security industry, in assessing the risk to a given computer application, begins with a “Threat Analysis” to define the types of security attacks to which a computer system might be vulnerable. This is a complicated analysis and the Ad Hoc Touch Screen Task Force does not possess the expertise, time or the resources to conduct a definitive and professional “Threat Analysis” of the entire voting process, but it may be appropriate for this analysis to be commissioned, funded, and conducted by others.

2. ADMINISTRATIVE SECURITY

FEDERAL TESTING - All voting equipment and systems used in elections in California are required to be tested by the federal and state governments. Initial qualification testing is done by an “Independent Testing Authority” (ITA) and uses guidelines adopted by the federal government for voting system performance and security. Both the hardware and software of voting systems are analyzed and tested.

There is general agreement on the Task Force that the federal testing standards and procedures should be substantially improved to enhance security and other aspects of voting equipment.

STATE TESTING AND CERTIFICATION - Once voting equipment has received federal qualification, it is eligible to apply for certification by the state for use in California elections. This certification process requires further testing by an internationally renowned voting systems consultant on contract with the state. This consultant conducts performance tests to ensure that the equipment is accurate and secure and can conduct elections according to California law. In addition, the applicant must demonstrate the equipment to election officials, interest groups (such as persons who are blind or visually impaired), and others. The applicant is currently required to place the source code that operates the voting system in an escrow facility and to produce an extensive manual of procedures for the use of the equipment. The voting system is considered for certification at a public meeting of the state's Voting Systems and Procedures Panel.

There is general agreement on the Task Force that the state process for certification and testing should be substantially improved to enhance the security and other aspects of voting equipment.

LOCAL TESTING AND PROCEDURES – Once a voting system is certified for use in California, local elections officials may purchase the system for use in their jurisdiction. Currently, there are several different technologies certified for use by the Secretary of State, including DRE systems, optical scan equipment (of multiple varieties), and punch cards (pre-scored punch cards will be decertified as of 2004). The choice of which voting system to use is made by each local jurisdiction (county or city).

When voting equipment is purchased, the local elections official is required to conduct "acceptance tests" on the equipment.

There is general agreement on the Task Force that the process of acceptance testing can be improved to enhance the security of the process.

At every election, all voting equipment is required to be tested by the local elections official conducting the election. This testing includes "Logic and Accuracy" testing, a process during which voting equipment is tested with a known number of votes and must produce exactly that result in order to be certified for use in the election. Once certified, it is sealed and if tampering occurs there are security procedures in place for the machine to be removed from service.

There is general agreement on the Task Force that Logic and Accuracy testing is essential for pre-election and post-election testing of voting equipment and provides substantial safeguards against error and machine malfunction. There is also general agreement that these tests can be improved.

3. VOTER CONFIDENCE

It is vitally important that all Californians have confidence in the integrity of the electoral process, including the equipment on which they cast their votes. Although the technology of voting is changing and becoming more and more computer based, all California voters should have confidence that elections officials and others are engaged in a process of continuous improvement to ensure that voting equipment keeps up with the challenges of new technology. The Task Force feels its recommendations should be considered with the understanding that California's testing and certification procedures are considered among the strongest in the nation, and DRE systems currently used in California are certified to conduct an accurate and reliable election.

4. VOTER VERIFICATION

The final issue examined by the Task Force is that of verification by the voter of his or her ballot.

The recently enacted federal Help America Vote Act of 2002 (HAVA) requires that each voting system "permit the voter to verify (in a private and independent manner) the votes selected by the voter on the ballot before the ballot is cast and counted." This is generally understood to mean that each DRE system should provide every voter with an opportunity to confirm his or her votes through an on-screen review of the voter's choices. This does relate to a voter verified paper audit trail (VVPAT), which would provide each voter a separate and additional opportunity to verify their selections by rereading those choices on a piece of paper.

HAVA also requires that each voting system "produce a permanent paper record with a manual audit capacity," and that the voting system "provide the voter with an opportunity to change the ballot or correct any error before the permanent paper record is produced."

This section is widely understood to mean that after voters confirm their votes via an on-screen review, and their ballots are cast, that a permanent paper record of each ballot be printed and kept by the local elections official in the case of a recount. HAVA is silent on whether this paper record should be printed concurrently with the on-screen confirmation, after the ballot is cast inside the machine, or at the end of the voting day once the polls close. And if printed concurrently with the voter's on-screen confirmation, HAVA does not speak to whether the paper record must be made available for each voter to verify their choices, or whether it should be printed inside the machine or at a separate printer without providing voter verification.

Currently there is one system certified in California that has a voter verified paper audit trail. This system allows a voter to review their choices using an on-screen display, and then to do a second confirmation on a printout which lists their voting choices. This printout can then be accepted by the voter, which casts the ballot, or rejected by the voter if the voter does not wish to cast those votes or if the voter believes there is a discrepancy between a vote they chose on the DRE screen and the vote shown on the printout.

The Task Force examined how the paper audit trail requirement should be accomplished, and whether the paper audit trail should be voter verified concurrent with the on-screen confirmation. A DRE system with a voter verified paper trail provides several security benefits in that it assures that the vote cast is accurate, and that any errors or inconsistencies between the DRE's electronic tally and the voter verified paper tally can be easily located and addressed.

However, voter verified paper audit trails impose greater administrative and technical needs, and so the Task Force also discussed voter verification options that do not involve paper.