# RECOMMENDATIONS

The Task Force has agreed that there are four major areas deserving recommendations to the Secretary: Security, Paper Records, Voter Verification, and Independent Verification.

## 1. SECURITY

There are currently too many holes in the federal qualification and testing process that need to be strengthened in order for the Task Force to be confident that software is being developed, checked, tested, loaded, and run with adequate safeguards to prevent tampering or bugs.

After hearing from experts on computer security as well as election experts versed in election administration security procedures, and receiving no response from several inquiries to Wyle Laboratories and Ciber (two of the three federal ITAs that test DRE voting system hardware, software and firmware), the Task Force agrees that each of these areas is not as strong as they can and need to be.

In addition, some members of the Task Force have significant concerns about the security protocols that vendors have in place during the product development phase and throughout the vendor's participation in the modification and improvement of software and systems through software patches.

As such the Task Force makes the following recommendations to improve security and testing procedures at all levels:

### A. Federal Testing

1. System security and integrity requirements must be more specifically defined at the Federal level. These requirements must assure a clean operating

environment both during the development process and during the operational phases while running an election, with no possibility of undetected intrusion at each point.

2. The ITA Qualification Tests must assure that the Federal requirements are met, to avoid duplication of testing effort by individual states.

3. A system designed to protect the most valuable aspect of our democracy – our voting systems, must be free from any questions over inadequacy, conflicts of interest, or collusion. Transparency is the only method that will ensure that the public does not question the intensity of the certification process. Therefore, the Federal testing process must increase transparency by incorporating citizen observation and participation and increasing public disclosure throughout the entire qualification process.

4. Testing of software and hardware is not a finite process. As technology evolves it becomes easier to hinder or intrude upon a system. Yet, software code in an election system that is tested at the Federal level, might be audited and tested once by an ITA, and if it passes and is never modified, may never be tested again. As such, the Federal testing and qualification process must allow for continuous improvement such as through periodic review and testing, instead of one-time testing.

5. Most current systems in California were certified using the Federal Elections Commission's 1990 standards, which were in place at the time of their certification. Earlier this year, new standards were adopted for the ITAs to use in testing election systems (known as the 2002 Standards). The Task Force agrees that all systems previously certified using the 1990 standards should be required to be retested by current standards. If a system certified under 1990 standards cannot meet the current standards, the Task Force would recommend that the state and federal governments provide funds to assist local jurisdictions in obtaining systems that are consistent with these standards. Such a replacement of the system should be done on a phased-in approach in order to avoid a problematic transition during an election.

6. Currently there is insufficient ongoing oversight of the ITAs to ensure that they are utilizing adequate quality control and maintaining the highest levels of scrutiny in testing election systems. The Task Force recommends that the National Institute of Standards and Technology (NIST), which the recently enacted Help America Vote Act of 2002 (HAVA) directs to establish federal standards, or the appropriate federal entity, conduct ongoing oversight of the ITAs.
7. Federal funding must be appropriated to enable NIST to conduct ITA oversight and to increase the technical security of systems.
8. Sometimes a large fraction of the software code, known as Commercial Off-The-Shelf (COTS) code because it is readily available for purchase to the public, is not audited at all. For systems without some form of voter verification, the blanket exemption for review of COTS code should be eliminated.
9. The Task Force recommends that NIST or the newly established Election Assistance Commission create a national database to track and document problems found in election systems, similar to Federal Aviation Administration incident reports, in order to keep local jurisdictions and the public informed.

**B. State Testing**

1. California certification tests are conducted or overseen by the Elections Division of the Secretary of State's Office. These certification tests must be focused on Elections Code and Election Division requirements. As such, the Election Division Regulations should assure that all ITA and NIST activities have been successfully completed as a prerequisite to certification testing.
2. The State should develop model Operational Security, Communications Security and Data Security procedures. Local jurisdictions should adapt the model procedures to their environments, and follow them in all elections operations.

3. When a vendor provides operating procedures for a system, they are often insufficient and incomplete. These operating procedures prepared by a vendor should include all operator functions required to assure proper operation in order to obtain certification.

4. Just as the Federal certification process must allow for continuous improvement such as thorough periodic review and testing, instead of one-time testing, so must the state certification process.

5. The Task Force acknowledges that its mission is limited by factors of time and knowledge. Therefore, the State should create a Technical Oversight Committee comprised of technical experts who can improve current testing and code-review standards, provide expert guidance throughout the certification process, and serve as a panel to review software and hardware issues that might arise. The panel members should be independent experts in computer science (especially computer security) and other engineering fields as appropriate who have technical expertise related to software development, computer security, user interface design, and other related fields. Panel members must not have financial or other conflicts of interest with voting equipment vendors. The panel should be convened by July 2003 and its meetings must be open to the public.

6. Like other states, California must require financial statements from applicants when they apply for certification.

7. The State must include a security analysis and a software analysis in its state certification.

8. The State must require the "threat analysis" from the federal ITA as part of all required documents before state testing of a vendor's system can begin.

9. To ensure that the code approved at the state and federal levels is identical to the code used at the local level, the State must require that the ITAs provide it with the executable code of each system to be tested. In addition,

the State must develop a system to compare that code with what a county uses on its machines for elections.

10. The State must obtain copies (either from the ITAs or from the vendors) of everything that each vendor provides to the ITAs, including source code, along with all the documents prepared by the ITAs during the Federal testing process. The Technical Oversight Panel (mentioned above in recommendation B(5)) should be able to review these documents at any time. All of these documents, except the source code and the threat analysis, would be public documents unless the vendor could establish that a document (or a potion thereof) meets certain standards of confidentiality or proprietariness established by the State, which would enable the document to be privileged. Those State standards should be made available to the public.

11. The State must conduct random audits of machines throughout the state to assure that software code in escrow with the State is the same code in use on each machine.

12. The State must conduct, or require local jurisdictions to conduct, random on-site sampling (otherwise known as “parallel monitoring”) of a specific number of machines on Election Day to confirm that each system in operation is registering votes accurately. The procedures must be created by the Secretary of State in consultation with the Technical Oversight Committee mentioned in recommendation B(5). Protocols must also be in place in case a discrepancy is determined so that each jurisdiction using that type of machine can be notified promptly in order to take questionable systems out of service and the State can initiate an investigation.

13. The State must make voting system procedures, which are often adopted administratively, easier for the public to find and access. This could include adopting these in regulation or some other alternative such as publishing a readily available procedures manual or placing procedures on the Internet.

## C. Local Testing

1. The integrity of the election process is based on the necessity, reliability, and comprehensiveness of the Federal and State certification procedures. As such, local jurisdictions that utilize systems that are not certified equipment or software must face State penalties.
2. State-approved communications security procedures are a pre-requisite to system-use in a live election. To ensure that hackers cannot intrude on a live system during voting, local jurisdictions must be on an isolated network. Furthermore, local jurisdictions should refrain from connecting voting machines to the Internet at any time.
3. The Logic and Accuracy process conducted at the local level must also be as reliable as the Federal and State tests. As such, the system vendor must not conduct these public tests.

## D. Distribution of Software

1. The distribution of qualified voting system software should be tightly controlled. NIST should distribute qualified object and source code to the State, and the State, not the vendors, should control the distribution of object code to the local jurisdiction using that system.
2. Voting system vendors should not be permitted to alter object code without retesting and re-certification.

## E. Technology

1. In order to minimize unintentional “undervotes,” voters must be provided with a review screen on all DRE systems that provide them a reminder that they have not voted in or have skipped a particular race. This must also occur on any additional equipment providing audio for those with visual disabilities, illiterate voters, and those with limited manual dexterity.

**F. Vendor Security**

1. In order to assure that vendors are using programmers and designers of software that have only a commitment to creating the best product, and to prevent easily foreseeable problems for individuals with a clear history of criminal activity and/or mental instability, the State must require vendors to conduct background checks of programmers and developers before they are not hired to work on election system software. The State should establish the standards for these background checks, and the results of the checks must be made available to the State upon request.
2. The State must establish protocols and procedures for vendors to comply with, in order to guarantee that strict internal security procedures are used during their software development process. And vendors should be required to submit employee security procedures with their certification materials.
3. Vendors should be required to document a clear chain of custody for the handling of software to assure that all software and storage units containing software are handled, tested and transported in an appropriate manner.
4. The State must impose civil liability and stiff criminal penalties if any malicious code is found before, during, or after certification, whether such malicious code interferes with an election or simply was intended to. The liability and penalties must apply to the programmer or developer of the malicious code as well as to the vendor employing the individual(s).

## 2. Printing a Permanent Paper Record

Both Proposition 41 and the federal Help America Vote Act of 2002 (HAVA), seem to require a paper audit trail be prepared for each polling place.

Section 301(2)(B)(i) of HAVA states that a voting system must produce "a permanent paper record with a manual audit capacity." In addition, HAVA states "this paper record shall be available as an official record for any recount conducted with respect to any election in which the system is used."

Section 19234(e) of the Elections Code as passed by Proposition 41 states that "Any voting system purchased using bond funds that does not require a voter to directly mark on the ballot must produce, at the time the voter votes his or her ballot or at the time the polls are closed, a paper version or representation of the voted ballot or of all the ballots cast on a unit of the voting system. The paper version shall not be provided to the voter but shall be retained by elections officials for use during the one percent manual recount or other recount or contest."

While it may seem that this section of law requires a paper audit trail be printed, this provision has not been interpreted that way. The Secretary of State's Office and the Voting Modernization Board, created by Proposition 41, have interpreted this provision to mean only that a system have the 'capability' to print a paper record. In other words, if a DRE collects ballot images on a memory card, and a paper record can be printed later from the memory card, this has been deemed acceptable.

The Task Force agrees that to provide this required permanent paper record for each election, each local jurisdiction not using VVPAT should print out each voter's ballot as a record of the vote shortly after the closing of the polls. This process should be open to viewing by the public. For technical and logistical reasons there is no support to have the printing of this permanent paper record done at the time the ballot is cast (unless the system allows the voter to verify his or her vote on paper). These technical reasons include the potential for printer jams or printer failure, and limited time to adequately train volunteer poll workers how to fix printers in the middle of a hectic election.

Therefore the creation of the permanent paper record, if it is not a VVPAT, should be done once all ballots are cast. For research and statistical analysis purposes, each

local jurisdiction should provide these per-precinct ballot images to the State, which should make them available on CD-ROM at minimal cost to the public.

The Task Force also agrees that on all DRE systems, whether it includes a VVPAT option or not, that the electronic vote should be the legally valid vote unless there is some sort of discrepancy between it and the permanent paper record. The paper record would be used for the 1% manual recount mandated by California law. Then, if there is a recount or a challenge, there would be a 100% recount of the paper record. For the 1% manual recount and a full recount, the paper record should be presumed to be more reliable than the electronic vote unless there is evidence it has been corrupted or is incomplete. This would be true of any paper audit record produced, whether voter verified or not.

## 3. Voter Verified Paper Audit Trail

The issue of whether election systems should contain a voter verified paper audit trail (VVPAT) was one of the key questions discussed and debated by the Task Force. There was no consensus on the issue of whether a VVPAT should be required on all systems certified in California.

The Task Force includes individuals who are strong advocates for requiring a VVPAT not only to guard against software discrepancies or malicious code from creating problems in recording ballot choices, but also to identify other type of events which could upset the ballot count.

These advocates explain that stakeholders in our voting system -- voters, candidates and political parties -- must believe the voting system is secure and accurate if they are to have confidence in election outcomes. A fundamental component of voting system security is the ability to conduct a reliable audit of the election.

The advocates for VVPAT argue that there are three key criteria required to conduct a reliable election audit. Not only must there be a permanent record of each voter's ballot maintained for a period of time after the election (see Recommendation #2 above), but voters must be able to verify the accuracy of this permanent record and the audit process must be transparent.

The advocates for VVPAT believe that voters must be able to verify the accuracy of the permanent record because only the voter knows the true intent of their votes and how they cast their ballots. The only time voters can verify the accuracy of their ballots is while voting because once a ballot is cast, ballots become anonymous. The audit process must be transparent so that the permanent ballot records are visible to election stakeholders.

The Task Force members advocating for a VVPAT further explain that if election security is to be accepted by a wide variety of stakeholders and the public is to maintain its confidence in elections, then the audit process needs to be a reliable method that is widely understood. They explain that the most well-known and tested method for meeting these criteria is a paper-based audit system.

Currently, paper is the most widely used and understood medium for protecting valuable documents and verifying important transactions, such as those dealing with money, property and legal matters. The Task Force members supporting a VVPAT claim that if the permanent ballot record exists in an electronic, rather than paper format, that the electronic record could be easily altered after it has been verified and therefore is not a permanent record. No audit medium is tamper-proof, but they believe that a paper audit trail is more permanent and transparent than a digital audit trail that depends on software not readily apparent or understandable to stakeholders, particularly voters.

A voter's ballot is one of the most important documents that exists in a free society. The advocates for VVPAT say that to entrust this document to an entirely computerized system run on proprietary software (protected by trade secret) with no voter verified

paper audit trail is to ask voters, candidates (winners and losers alike) and parties to exercise blind trust in the voting system. Therefore, they feel that given the limitations of current technology, a voter-verified, paper audit trail is the only proven way to mitigate the real (and perceived) security risks inherent in any computerized voting system, such as programming errors, the use of unauthorized software, and deliberate attempts to manipulate an election.

Other Task Force members, though, are opposed to requiring a voter-verified paper audit trail because they argue that there are significant limitations on its implementation such as legal, technical and administrative constraints on how a VVPAT system would need to be designed.

Members of the Task Force opposing VVPAT suggest that printers add an increased technical burden at the polls since printers are often problematic, requiring on-the-spot troubleshooting during an election in the case of a problem. There are also added costs imposed on the State and counties to purchase, maintain and store printers, as well as to provide printing supplies.

In addition, those opposing a VVPAT requirement argue that there are legal burdens imposed on the design of each VVPAT system. For instance, HAVA requires that voting systems provide individuals with disabilities (especially the visually impaired) "the same opportunity for access and participation (including privacy and independence) as for other voters" and California Assembly Bill 2525 (Jackson), Chapter 950, Statutes of 2002, requires that blind voters be provided with "access that is equivalent to that provided to individuals who are not blind."

In addition, Section 2.2.7.2 of the Federal Election Commission's new 2002 standards specifies "DRE voting systems shall provide, as part of their configuration, the capability to provide access to voters with a broad range of disabilities. This capacity shall…provide audio information and stimulus that…provides instruction so that the

voter has the same vote capabilities and options as those provided by the system to individuals who are not using audio technology."

The opponents of requiring VVPAT argue that it is questionable whether providing a piece of paper to sighted voters to verify their choices while not providing a similar chance for verification for those with disabilities can be seen as "the same opportunity for access and participation (including privacy and independence) as for other voters," as "equivalent" access, or as "the same vote capabilities and options." Therefore, it remains an open question whether a VVPAT can be made to conform to these laws.

In addition, language access is also an issue since verification for non-English language voters would need to be in their preferred language. This can be difficult to accomplish while also ensuring that if a recount occurs the ballot can both be read by election officials and allow for secrecy (since there may be few voters casting ballots in that language). Printing bilingual ballots eases the readability issue, but does not address the secrecy issue. It also lengthens the size of the paper needed for verification.

Therefore the Task Force arrives at no consensus on the question of whether a voter verified paper audit trail (VVPAT) should be required. However, the Task Force agrees that systems with a VVPAT should be an option for local jurisdictions to choose, if such systems can meet the language accessibility requirements of HAVA, and the disability accessibility requirements of HAVA, AB 2525 and the FEC's 2002 standards.

For jurisdictions that choose to utilize systems with a VVPAT, there are several issues that must be addressed in order to give greater clarity to vendors, election officials and the public. The Task Force recommends that the state's Voting Systems and Procedures Panel, which is the state certification advisory body, address a series of issues related to VVPAT to ensure that all vendors utilizing such an option are conforming to consistent standards, and that conformity be a prerequisite of certification.

The issues to be addressed include, but may not be limited to, the following:

- ❑ Assuring randomized out-stacking of the paper ballot copies.
- ❑ Requiring adequate storage space and paper supply in each voting unit in order to accommodate the large number of ballots cast (and spoiled ballots) by the maximum number of voters allowed for each voting unit.
- ❑ Establishing design criteria for the paper ballot copies such as being easy for the voter to read, being in a format that lends itself to easy counting after the election, and determining the specific information to be included on the paper ballot copy.
- ❑ Establishing procedures that allow voters to reject or "spoil" their paper ballot copies.
- ❑ There will need to be procedures developed to enable voters who notice discrepancies to alert the precinct's poll workers. Such procedures would also need to stipulate under what conditions a voting machine would have to be taken offline.

## 4. Alternative Verification Methods

Because of reservations about paper-based voter verification, the Task Force wanted to encourage the development of alternative voter verification technology, such as fully electronic verification, that would ensure the security of each vote as well as provide greater voter confidence. Many (but not all) technologists feel that such alternatives could be developed and deployed within the next few years. The Task Force suggests that the State should explore urging, incentivizing, and possibly requiring vendors to develop such methods.

Until such time as alternative voter verification technology is readily available, voter confidence can be increased by following recommendation 1(b)(12) made earlier in this report regarding random on-site sampling of machines on Election Day (also known as Parallel Monitoring). Election Day sampling far exceeds the current testing methods in

use in California and elsewhere, and has a strong likelihood to detect potential machine tampering. The recommendation that each local jurisdiction make per-precinct ballot images available will also allow powerful post-election statistical analysis, which can provide evidence that even elections with surprising results reflect the will of the voters.

Because of the increased protections imposed by Election Day sampling, the Task Force agreed that there is time for vendors to develop voting systems with alternative voter verification of a ballot cast without paper. Electronic verification methods should preferably be within the machine to minimize extra equipment, and should not delay the time it takes to vote. The system should also be as voter friendly as possible and minimize any inconvenience or confusion to the voter. If feasible, it should provide the existing user interfaces while seamlessly including verification within the machine with little or no additional steps for voters to apply.

The Task Force agreed that there needs to be voter verification imposed by a date certain and the State and federal governments must provide funding to make this happen. There was disagreement, though over what type of voter verification audit mechanism to require, and on what timeline.

Six members of the Task Force would require an electronic verification method. These members believe that the technology is very close to developing an electronic voter verification audit mechanism for DREs that would not utilize paper. But these Task Force members want to provide enough time for the market to meet that need. They felt that it will take some time to perfect electronic verification audit methods, for these methods to be integrated into DREs, and for these methods to be federally qualified, state certified, and mass produced.

As such, this group of Task Force members recommends that the State allow vendors until December 31, 2006 to develop and obtain certification for such a solution, and at that point restrict vendors' ability to sell DRE systems without an electronic verification

feature. Therefore, all new systems purchased and put into use from January 2007 on must include an electronic verification audit feature that does not utilize paper.

But due to cost and the potential to create chaos in our electoral process, these members believe that the State should phase-in compliance for all jurisdictions that purchased DREs before 2007. And that all voting systems purchased prior to 2007 should be replaced with systems containing electronic verification or upgraded to include such a verification feature by 2010.

Three remaining Task Force members strongly agree with the idea of a voter-verified audit trail requirement (either with alternative verification or a voter verified paper audit trail), but feel a much greater sense of urgency about the timing of the conversion. This group feels that the state should impose such a requirement immediately, and that no additional DRE voting equipment should be purchased unless it meets that requirement. Counties that need to upgrade have several options available, including optical scan systems and DREs with printers (one such system is currently certified, and additional ones may be certified soon).

If a voter verified audit trail requirement is not imposed immediately, this group feels that it is vital that any new purchases of DREs be planned and budgeted with the conversion to this requirement in mind. To achieve this, this group believes that the State should mandate a voter-verified audit trail requirement (either with alternative verification or a voter verified paper audit trail), by January 2007 for all equipment deployed from now on (this deadline could be extended until 2010 for DREs currently in use). In addition, the state should strongly encourage all counties moving to deploy DRE voting systems to implement the requirement as soon as possible in advance of the deadline. Counties should negotiate those upgrades into their contracts, as Santa Clara County did in the contract signed at the end of April 2003, so that any additional costs due to the voter verified audit trail requirement can be covered by current Prop. 41 and HAVA funds.

This group is greatly concerned about the number of new purchases of DRE systems that are scheduled to occur before 2007. These Task Force members argue, that with these planned purchases, the number of California voters living in counties using DREs is expected to increase from about ten percent to over 50 percent by 2007. If a voter verification requirement does not take effect until 2010, this expansion will expose a majority of California voters' ballots to what these Task Force members believe to be serious security risks over the course of several major election cycles.

These Task Force members worry that if current plans come to pass, hundreds of millions of dollars of State and Federal funds will be expended on equipment that does not meet the proposed requirements. In 2010, the State will be faced with potentially large expenditures for upgrades. This cost may be so great that the voter verified audit requirements will be further delayed.

Therefore, the Task Force members are not far apart on imposing verification for all DRE systems in California – 3 years – and not far apart on the types of verification - with all members encouraged by the possibility of electronic or alternative verification methods, but three members believing that paper –based voter verification should be required immediately until electronic or other alternative voter verification methods are feasible.

All members also agree that prior to state certification testing, conformance with the electronic independent audit requirements should be determined by the Voting Systems and Procedures Panel, in consultation with the Technical Oversight Committee mentioned above. Before and after equipment has been acquired, the Voting Systems and Procedures Panel, in consultation with the Technical Oversight Committee, should have the power to ensure the integrity of verification audit mechanisms by ordering independent technical evaluations of voting equipment (including equipment that has already been fielded) at the expense of the vendor.

All information that the panel uses to arrive at its judgment on these audit mechanisms, including all design details of the audit mechanisms, including source code for any software they use, should be made public. The conclusions of the committee and the justifications for those conclusions must also be made public.

All the members also agreed that it is imperative that voter confidence in voting systems currently in use not be eroded by our efforts to add additional layers of security to the process. As such mechanisms are developed and certified, any adoption must be through careful integration into existing systems or part of system replacements and/or upgrades. Any state-mandated incorporation of independent electronic verification on existing systems must include full funding by the State or federal government for all costs.