Secretary of State's

Ad Hoc Touch Screen Task Force

Report

SECRETARY OF STATE **KEVIN SHELLEY**

July 1, 2003

TABLE OF CONTENTS

INTRODUCTION

Secretary of State Kevin Shelley created the Ad Hoc Touch Screen Task Force on February 19, 2003 in response to concerns expressed over the security of DRE voting equipment. The purpose of the Task Force was to study these concerns, discuss possible improvements, and to make recommendations to the Secretary of State and the Voting Systems and Procedures Panel.

The Task Force is comprised of individuals who brought vastly different backgrounds, experience, and views on these issues. Over the course of eight meetings, the Task Force heard from the Secretary of State, local election officials, voting system vendors, experts in computer security, a representative of an independent testing authority, a representative of the NASED ITA Technical Subcommittee of the Voting Systems Board, and representatives of the disabled and civil rights community.

This report represents a consensus view on the issue. However, with such diverse backgrounds and such a limited time to provide recommendations, it is clear that this committee has not made recommendations on every aspect of this issue. As such, we have provided a range of options with an explanation for each.

The Task Force is comprised of the following individuals:

Mark Kyle, Undersecretary of State (Chair)
Marc Carrel, Assistant Secretary of State for Policy & Planning (Co-Chair)
Kim Alexander, Founder and President of the California Voter Foundation
David Dill, Professor of Computer Science, Stanford University
David Jefferson, Computer Scientist, Lawrence Livermore National Laboratory
Robert Naegele, President, Granite Creek Technology, Inc.
Shawn Casey O'Brien, former Executive Director, Unique People's Voting Project
Mischelle Townsend, Registrar of Voters, Riverside County

Charlie Wallis, Department IT Coordinator, San Diego County Registrar's Office
Jim Wisley, Office of Assembly Speaker Herb Wesson

In addition, the members of the committee would like to thank the efforts of John Mott-Smith, Dawn Mehlhaff, Bruce McDannold, Debbie Parsons, and Terri Carbaugh of the Secretary of State's Office, and InfoGard Laboratories for their assistance to the Task Force.

EXECUTIVE SUMMARY

Secretary of State Kevin Shelley created the Ad Hoc Touch Screen Task Force on February 19, 2003 in response to concerns expressed over the security of Direct Recording Electronic (DRE) voting equipment. The purpose of the Task Force was to study these concerns, discuss possible improvements, and to make recommendations to the Secretary of State and the Voting Systems and Procedures Panel.

In March of 2002 California voters enacted the Voting Modernization Bond Act, establishing a fund of $200 million for counties to upgrade their voting equipment. In 2002 the federal government enacted the Help America Vote Act requiring election reform and providing funds to, among other things, have at least one voting machine in each polling place that is accessible to the blind and visually impaired. The same year, the State enacted AB 2525 (Jackson), Chapter 950, Statutes of 2002, requiring voting equipment be accessible to persons with visual disabilities when a county purchases new voting equipment.

These laws and a federal court order created an incentive for counties to purchase DRE voting equipment (which includes touch screen voting systems) and move away from paper ballots and earlier mechanical voting systems. This has led some members of the public to raise concerns regarding the security of the DRE systems. Essentially, the argument is that DRE voting equipment relies on a “black box” computer with proprietary source code and object code hidden from the public, and therefore the potential exists for unknown reliability and security risks.

The public discussion of the security of touch screen voting equipment has primarily focused on the issue of a “paper trail” or paper audit trail, and whether (and what type) would be necessary to back-up the electronic record of the vote. While there exists a paper audit trail requirement in state and federal law, some have advocated this be a “voter verified” paper record so voters can verify their choices on paper before their ballots are cast. Other audit methods have also been discussed.

These issues are at the core of what the Ad Hoc Touch Screen Task Force was constituted to address. The four key issues addressed by the Task Force were: (1) Computer Security: Whether there is evidence of a security issue with DRE voting systems and, if so, the nature and probability of the security issue ; (2) Administrative Security: Whether the existing federal, State and local tests are adequate, and whether current security protocols and processes used by DRE vendors are adequate; (3) Voter Confidence: How to ensure voter confidence in our voting systems and elections; and (4) Voter Verification: Whether verification by voters is useful or not; whether verification by voters is necessary or not?

After examining these questions, the Task Force examined the many legal, technical and procedural constraints which surround them. These include: (1) Federal and state laws involving the accessibility of the blind or visually impaired voters, voters with no or low literacy, and those who do not speak English; (2) The court ordered replacement of punch card voting systems in California; (3) Challenges affecting the development of new or improved products and the federal and state testing process required; (4) Efforts to create problems by imposing new mandates or burdens too quickly, which could detrimentally impact the 2004 elections; (5) Issues involving the administration of elections; (6) Issues related to printers; (6) The realities of the marketplace; and (7) The cost to implement any solution recommended and the requirement that such costs could be borne by the State.

FINDINGS

The following are the major findings of the Task Force:

- *Voting equipment should and must meet the requirements of federal and state laws requiring access to voting.*

- *The time requirements for product development and certification are significant issues in terms of the timing of the development of potential market solutions to address any of the issues brought up in this report.*

- *Any recommendations to change current voting equipment recognize the paramount importance of a successful election in terms of voter confidence, and no recommendations should be utilized to undermine the successful administration of those elections.*

- *Any proposed method of verification must not inconvenience voters, create lines at the polling place, or otherwise discourage voters from casting a ballot.*

- *Any new equipment options should be as simple to administer as possible so as to not create unnecessary complexity at the polling place.*

- *There are a number of logistical challenges that are present with any paper-based voting system using printers and these challenges need to be explored and understood in greater detail.*

- *Local jurisdictions, if they desire independent verification on their systems, should have a range of verification options to choose from, including paper-based and electronic options.*

- *State or federal funds should be provided to pay the cost of upgrading any system that does not meet the requirements implemented as a result of the recommendations of this report.*

- *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.*

RECOMMENDATIONS

Based on these findings and after hearing testimony from a wide range of experts, the Task Force agrees that there are four major areas deserving recommendations to the Secretary: Security, Paper Records, Voter Verification, and Independent Verification:

1. SECURITY

FEDERAL TESTING - 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.

The Task Force offered nine recommendations to improve the federal testing process *(see pages 27-29)*. These include:

- Opening up the federal testing process to citizen observation.
- Altering the Federal testing and qualification process from a one-time testing process to an ongoing process involving periodic review.
- Making sure that all systems in use in California are retested under the most current federal standards.
- Charging the National Institute of Standards and Technology (NIST) with conducting ongoing oversight of the Independent Testing Authorities (ITAs)

- Providing federal funding to enable NIST to conduct ITA oversight and to increase the technical security of systems.
- Removing the blanket exemption for testing of Commercial Off-The-Shelf (COTS) software for systems without voter verification.
- Establishing a national database that is maintained at the federal level to track and document problems found in election systems in order to keep local jurisdictions and the public informed.

STATE TESTING- 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. The Task Force makes 13 recommendations to improve the State testing process *(see pages 29-31)*. These include:

- Assuring that all ITA and NIST activities have been successfully completed as a prerequisite to certification testing.
- Developing model Operational Security, Communications Security and Data Security procedures to be adopted for use by local jurisdictions.
- Requiring vendors to provide complete operating procedures in order to obtain certification.
- Altering the State certification process from a one-time testing process to an ongoing process involving periodic review.
- Creating 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 review software and hardware issues.
- Requiring a “threat analysis” from the federal ITA as part of all required documents before state testing of a vendor’s system can begin.
- Ensuring that the software code approved at the state and federal levels is identical to the code used at the local level, by requiring the ITAs to

provide the State with the executable code of each system to be tested and to develop a system to compare that code with what counties use on their machines.

- Obtaining copies of everything that each vendor provides to the federal testers, including source code, along with all the documents prepared during the Federal testing process. All of these documents, except the source code and the threat analysis, would be public documents unless the vendor could establish that a document meets certain public standards of confidentiality or proprietariness established by the State, enabling the document to be privileged.
- Conducting random audits of machines throughout the state to assure that software code held by the State is the same code in use on each machine.
- Conducting 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.
- Making voting system procedures easier for the public to find and access.

LOCAL TESTING AND PROCEDURES –There is general agreement on the Task Force that the process of acceptance testing can be improved to enhance the security of the process. There is also general agreement 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, but these tests can also be improved. The Task Force makes three recommendations to improve the local testing process *(see page 32)*.

- Creating penalties for local jurisdictions that utilize systems that are not certified.
- Protecting systems from hackers by requiring local jurisdictions to be on an isolated network and to refrain from connecting voting machines to the Internet at any time.

- Preventing the system vendor from conducting the Logic and Accuracy tests on a voting system.

DISTRIBUTION OF SOFTWARE and TESTING – To ensure the security of systems when traveling between entities and to ensure that a voter has not missed a selection, the Task Force makes three recommendations in these areas *(see page 32)*.

- 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.
- Restricting voting system vendors from altering object code without retesting and re-certification.
- Requiring a review screen on all DRE systems in order to minimize unintentional "undervotes," which must also be included on any audio accessories available for those with visual disabilities, low literacy, and limited manual dexterity.

VENDOR SECURITY - In order to assure that the internal security systems are improved, the Task Force makes four recommendations *(see page 33)*.

- Requiring vendors to conduct background checks of programmers and developers using standards established by the State.
- Establishing strict internal security protocols and procedures for vendors to comply with during their software development process.
- Requiring vendors to document a clear chain of custody for the handling of software.
- Imposing 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), require a paper audit trail be prepared for each polling place. This is separate and apart from whether this paper audit trail is provided to the voter to verify his or her vote before their vote is cast.

The Task Force agrees that to provide this required permanent paper record, that each local jurisdiction not using a voter verified paper audit trail, 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). Each local jurisdiction should also provide per-precinct ballot images to the State, which should make them available to the public on CD-ROM.

The Task Force also agrees that on all DRE systems, the electronic vote should be the legally valid vote unless there is some sort of discrepancy between it and the permanent paper record. For the mandated 1% manual recount or in the case of 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.

3. VOTER VERIFICATION

There was no consensus on the issue of whether a voter verified paper audit trail (VVPAT) should be required on all voting systems certified and used in California. However, the Task Force did agree that systems with a VVPAT should be an option for

local jurisdictions to choose, if such systems can meet the disabled and language accessibility requirements of State and federal law.

In addition, for jurisdictions that choose to utilize systems with a VVPAT, the Task Force recommends that the state's certification advisory body, the Voting Systems and Procedures Panel, , review and address a series of issues related to VVPAT to ensure that all vendors utilizing such an option are conforming to consistent standards.

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. The Task Force suggests the State explore the development of such methods.

Because of the increased protections imposed by Election Day sampling, the Task Force agreed that there is time for vendors to develop alternative voter verified audit methods. But 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, but they feel it will take some time to perfect a version a federally qualified, state certified, and mass produced version that can be integrated into a DRE. As such, this group recommends 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. All voting systems purchased prior to that date should be modified to include electronic verification by 2010.

Meanwhile, three Task Force members believe strongly that the state should impose a voter verification audit requirement immediately, and that no additional DRE voting equipment should be purchased unless it meets that requirement. This group is greatly concerned about the number of new purchases of DRE systems that are scheduled to occur before 2007. 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.

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.

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.

CONCLUSIONS

The Task Force members urge the Secretary and others to consider these recommendations and, given the importance that accurate election results are to our democracy, to seek their implementation at the local, state and federal levels. The Task Force recognizes the potential cost of implementing these recommendations, but urges the federal and state governments to make the necessary financial commitment.

BACKGROUND AND OVERVIEW

For the last 40 years, Californians have primarily voted on mechanical voting equipment using paper ballots that require the voter to either punch a hole in a card to indicate a vote selection, or to mark the ballot with a marking device. After the polls were closed, these ballots were collected from polling places and brought to a central location for counting.

The presidential election in Florida in 2000 focused attention on the weaknesses of paper ballots, including “chad” and the difficulty of establishing voter intent. The newspapers were full of pictures of election officials holding ballots up to the light to see if they could determine if the “pregnant chad” meant that the voter intended to punch a hole and cast a vote or not.

As a result of the difficulties experienced in that election, election professionals began examining the advantages of direct recording electronic (DRE) voting equipment (this category includes touch screens) and there was a movement away from using paper ballots. The advantages of DRE systems include: (1) no “chad”; (2) eliminating the possibility of an “overvote” (or making more selections than permissible) and advising the voter of any “undervote” (when a voter makes fewer than the maximum number of permissible selections in a contest); (3) providing persons who are blind, visually impaired or physically disabled with the opportunity to cast a secret ballot without assistance; (4) facilitating “early voting” and thereby encouraging greater voter participation; (5) eliminating marking devices which can result in questions of voter intent, and (6) providing a review screen before a voter casts a ballot.

In February of 2002 a federal judge ordered that all pre-scored punch card voting equipment in use in California be replaced not later than January 1, 2004. This order requires Alameda, Los Angeles, Mendocino, Sacramento, San Bernardino, San Diego, Santa Clara, Shasta, and Solano counties, home to 56% of the state’s voters, to convert to new voting systems.

The election in Florida in 2002 illustrated additional problems, notably the difficulty of converting to a new voting system, and the potential to disenfranchise voters if poll workers are poorly trained in the operation of new voting equipment. Reports following this election indicate that one of the principal reasons for problems was the lack of smaller local elections prior to a major statewide election in which to work out any technical and procedural bugs in the new systems and to train poll workers and voters how to use the new equipment.

In March of 2002 California voters enacted the Voting Modernization Bond Act, establishing a fund of $200 million for counties to upgrade their voting equipment. This provided a strong incentive, and momentum, for even more counties, in addition to the nine counties required by the court order, to also convert to new voting systems.

In October of 2002 the federal government enacted the Help America Vote Act requiring election reform and providing funds to, among other things, have at least one voting machine in each polling place that is accessible to the blind and visually impaired.

Also in 2002, the California Legislature enacted AB 2525 (Jackson), Chapter 950, Statutes of 2002, requiring that voting equipment be made accessible to persons with visual disabilities when a county purchases new voting equipment with Voting Modernization Bond Act or Help America Vote Act funding.

As a result of these new laws, California and other states began to purchase and install DRE voting equipment. To date, Alameda County, Plumas County, and Riverside County have converted entirely to DRE voting equipment. Several other counties are either testing DRE equipment in “early voting” environments, using it for smaller city elections, or are in the middle of contract negotiations to purchase these systems.

As elections officials have moved away from the earlier mechanical voting systems, some members of the public have raised concerns regarding the security of the new

DRE systems. Essentially, the argument is that DRE voting equipment relies on a “black box” computer with proprietary source code and object code hidden from the public, and therefore the potential exists for unknown reliability and security risks such as insertion of malicious code by an insider at a voting equipment vendor to manipulate the software of these machines in a way that would not be detectable and could affect the outcome of one or many elections simultaneously.

The public discussion of the security of touch screen voting equipment has focused primarily on the question of what kind of “paper trail” or paper audit trail is necessary to back-up the electronic record of the vote. In particular, apart from an existing paper audit trail requirement in state and federal law, some have advocated a “voter verified” paper trail – a paper record of the voter’s choices that the voter can use to verify his or her vote choices before casting their ballot or otherwise stored as a check against manipulation, fraud or error.

Although the public discussion has focused primarily on a voter verified paper trail as a means of further protecting against fraud or error, it is important to acknowledge that this protection can probably also be provided through an internal electronic audit mechanism. In addition, other procedural safeguards are available to increase detection of attempts to manipulate the accuracy or integrity of the voting system.

These potential security issues are the core of what the Ad Hoc Touch Screen Task Force was constituted to address, and the details of these issues are enumerated in the “Security Issues” section of this report below.

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.

LEGAL, TECHNICAL, AND PROCEDURAL CONSTRAINTS

As the Task Force discussed the issues of computer security, administrative security, voter confidence and voter verification, it became clear that several of these issues faced legal, technical and/or procedural constraints which posed, if not limitations, than at least some more questions.

1. FEDERAL AND STATE LAWS: ACCESSIBILITY FOR THE VISUALLY IMPAIRED, NO/LOW LITERACY VOTERS AND NON-ENGLISH SPEAKERS

Perhaps the most significant issue facing the development of any new voting system is the requirement in federal and state law that voting equipment provide blind and visually impaired voters with the ability to vote a secret ballot independently and without assistance.

The United States Congress, and the Legislature of the State of California, in enacting these requirements, clearly stated that this is a top priority and stipulated that federal and state funding shall be contingent on meeting this condition. In other words, the state, if it were to implement a ballot verification process that is not verifiable by blind voters, could place at risk the approximately $200 million the federal government is providing California for upgrading voting equipment and reform of the election process.

For all voting systems currently certified by the state, none has a paper-based voter verification option that can be utilized by blind, visually impaired, and illiterate or marginally literate voters, although several vendors have expressed the belief that such a process is feasible. Among the options vendors are exploring includes utilizing a fixed text reader that translates text to speech as the paper ballot is printed, or a reading pen

that would allow a blind voter to scan a pen across the paper print-out and hear the words spoken via a speech synthesis component in the pen.

Federal law also requires jurisdictions in California to produce election materials in languages other than English. The County of Los Angeles, for example, is required to provide ballots in English, Spanish, Chinese, Vietnamese, Tagalog, Japanese, and Korean. And Riverside County has a Cahuilla language requirement that is strictly an oral language and has no written form. Providing a paper-based representation of ballots in all these languages is also an important issue, as is the question of whether the paper-based representation must represent the ballot in English as well as the second language so that election officials can read the document.

The Task Force agrees that voting equipment should and must meet the requirements of federal and state laws requiring access to voting.

2. COURT ORDERED CONVERSION

A federal court order on the Secretary of State to assure that there are no pre-scored punch card systems in use in California beyond January 1, 2004, means that nine of California's counties must replace their punch card voting systems by that date. This can only be accomplished in conjunction with legal requirements for contracting and purchasing and the time limitations on state and federal certification of voting systems. For example, as of now, no voting systems currently certified by the state that provide for voting secretly and independently by persons who are blind include a voter verification option that the blind can utilize.

The Task Force agrees that the conversion process required by the presidential elections in 2004 must not be compromised and that its recommendations not undermine the successful preparation and administration of the upcoming March 2, 2004 primary election.

3. PRODUCT DEVELOPMENT AND TESTING CHALLENGES

In order for a county to purchase a system, the vendor would first have to develop it, submit it to national testing laboratories for security and other testing, and submit it to the state for similar testing and evaluation. In addition, the counties would have to issue Requests For Proposal, accept bids, analyze the bids, and negotiate a contract. Many counties are implementing a new voting system for local elections in November of 2003, only six months from the date of this report.

The Task Force agrees that the time requirements for product development and certification are significant issues in terms of the timing of the development of potential market solutions to address any of the issues brought up in this report.

4. DISASTER AVOIDANCE

Implementation of a new voting system requires – in order to avoid the missteps in the Florida 2002 election – significant time to train county personnel, train poll workers, educate the voters concerning the new voting systems, and otherwise prepare for the election. The likelihood that all of the steps outlined above could be accomplished in time to successfully install the equipment and successfully conduct an election in November 2003 is extremely remote.

The Task Force agrees that the presidential elections in 2004 must not be compromised, that any recommendations to change current voting equipment recognize the paramount importance of a successful election in terms of voter confidence, and that its recommendations not undermine the successful administration of those elections.

5. VOTER ISSUES

The California Constitution requires that voting be secret. Voting systems that rely on a "reel to reel" paper tape potentially order ballots sequentially, and could be amenable to efforts to determine which voter cast which ballot. In addition, in the absence of additional voting stations, there is the potential for increasing the time it takes to vote, creating longer lines at polling places, and discouraging voters from casting ballots.

There is unanimous concern on the Task Force that any proposed method of verification not inconvenience voters, create lines at the polling place, or otherwise discourage voters from casting a ballot.

6. ELECTION ADMINISTRATION

The recruitment and training of nearly 100,000 mostly elderly poll workers for a statewide election is a major undertaking under current circumstances. Requiring more complex equipment naturally raises concerns over poll worker recruitment, training, mechanical reliability, ongoing operational costs, and voter frustration. These concerns need to be considered.

The Task Force agrees that new equipment options should be as simple to administer as possible so as to not create unnecessary complexity at the polling place.

7. PRINTER ISSUES

One method discussed is to create a paper record of the vote for each voter to verify his or her ballot choices. This requires that a printer be added to the voting machine. The voting machine can produce the printed version of the ballot when the voter casts his or her ballot, when the polls close, or as required for the 1% manual recount. The latter two of these options are currently available on California-certified DRE systems.

Printers at polling places potentially create several significant election administration problems, including: (1) added cost to the system; (2) printer jams or other malfunctions requiring poll worker intervention; (3) added weight to the voting equipment; (4) current inaccessibility of the paper verification option to persons who are blind, visually impaired, illiterate, marginally literate, or are oral language restricted; (5) need for printers to print in foreign language characters; (6) more equipment that poll workers need to be trained to use and troubleshoot any problems; (7) more equipment for each jurisdiction to store, transport and maintain; and (8) additional supplies and warehousing procedures required to account for "official" ballot paper requirements.

The Task Force agrees that there are a number of logistical challenges that are present with any paper-based voting system using printers and these challenges need to be explored and understood in greater detail.

8. MARKETPLACE

As noted, there are currently no voting systems that offer paper-based voter verification procedures that provide persons who are blind or visually impaired with the ability to verify their ballot. Systems currently available, either as certified systems or as prototypes, rely on paper for a voter to verify the electronic record. The marketplace is potentially capable of addressing the technical issues with printers and poll workers listed above as well as producing solutions to achieving voter verification without utilizing paper.

The Task Force agrees that local jurisdictions should have a range of verification option to choose from, including paper-based and electronic options.

9. REIMBURSEMENT

As mentioned above, several counties have already purchased DRE voting equipment. New standards have been developed by the FEC and newer standards may be

developed by NIST. This presents potentially significant issues of funding and reimbursement, and raises the issue of the timing of any requirement for implementing new standards or acquiring new equipment.

The Task Force agrees that state or federal funds should be provided to pay the cost of upgrading any system that does not meet the requirements implemented as a result of the recommendations of this report.

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.

CONCLUSIONS AND NEXT STEPS

The Task Force spent many hours exploring these issues and seeking to arrive at recommendations that were both responsible and feasible. Everything in this report is designed to increase the security of voting systems as well as to increase the confidence of the voters.

While there was not agreement on every issue the Task Force examined, we urge the Secretary, the members of the Voting Systems and Procedures Panel and others interested in the design, use, and security of voting systems to consider our recommendations, as all of them are the consensus of a committee that was incredibly diverse in our experience with voting systems, and our perspective on these issues.

We urge the Secretary to carefully review this report and to strongly urge the federal testing and standards authorities to consider our recommendations to improve the federal testing and qualification standards.

The Task Force also encourages the vendor community to review their security procedures – not only within the systems they are producing, but also the vendors' internal production and development security protocols, to make sure these are as strong as necessary given the importance that accurate election results are to our democracy.

Finally, we are quite cognizant that many of these recommendations will take substantial time and money to implement. We urge the federal and state governments to consider the considerable value that our society places on fair and accurate

elections, and to make an equivalent financial commitment over the necessary time period.

APPENDIX: Glossary of Terms

Acceptance Testing – the examination of voting systems and their components by the purchasing election authority in a simulated use environment to validate performance.

Accessibility – The ability of the voting system to be independently utilized by individuals with disabilities including those who are blind or visually disabled, without compromising the voter's privacy or secrecy of his or her ballot. The ability of the voting system to be independently utilized by individuals with alternative language needs pursuant to section 203 of the Voting Rights Act of 1965.

Accuracy – precision in recording, calculations and outputs.

Alternative Voter Verification – voter verification of a ballot cast using non-paper media (e.g. electronic voter verification).

Ballot Image – the detailed record of the selections made by a particular voter.

Certification Testing - the examination and testing of a voting system to determine its compliance with state laws and requirements for voting systems.

Commercial Off-The-Shelf (COTS) – software products as elements of larger systems that are readily available for sale by the public.

Data Security – the various methods and procedures, such as the use of passwords and encryption, implemented to prevent unauthorized use, destruction, or disclosure of data, whether accidental or deliberate.

Direct Recording Electronic (DRE) Equipment – an electronic voting device that captures votes/ballots at the point at which they are cast by the voter. This category includes all touch screen devices.

Early Voting – a form of absentee voting in which any voter may vote at the office of the elections official or at a satellite location as determined by the local elections official.

Election Assistance Commission (EAC) – established, as a result of the Help America Vote Act of 2002, to serve as a national clearinghouse and resource for the compilation of information and review of procedures with respect to the administration of federal elections.

Electronic Voter Verification – non-paper voter verification of a ballot cast, which utilizes trustworthy hardware (and possibly software) independent from the main vote capture program in order to provide independent confirmation of a voters' selections.

Escrow – the process by which a third party, having no direct or indirect financial interest with a vendor, holds the voting system software source code, including all changes or modifications and new or amended versions, for safekeeping and possible verification.

Federal Election Commission (FEC) – the body formerly responsible for producing the Federal Voting Systems Standards (FVSS). Its duties are now being separated and most of its voting functions will be assumed by the new Elections Assistance Commission (EAC).

Federal Voting Systems Standards (FVSS) – contains all the requirements for independent testing of voting systems.

HAVA – see Help America Vote Act of 2002.

Hardware – the mechanical, electrical and electronic assemblies, including materials and supplies, which are a part of the voting system. Hardware includes the voting device on which individual voters cast their ballot, as well as the actual equipment used to program ballot software or central vote tabulation software.

Help American Vote Act of 2002 (HAVA) – the federal election modernization law enacted in October 2002 which attempts to set national standards for elections and provides funding for the replacement of punch card and lever voting systems.

Independent Testing Authority (ITA) – testing laboratories, which can perform testing related to voting systems to meet the FVSS.

Logic and Accuracy (L&A) – the tests conducted to ascertain that the system will count properly the votes cast for all contests.

National Association of State Election Directors (NASED) – selects and approves testing laboratories which can perform testing related to voting systems to meet the FVSS.

National Institute of Standards and Technology (NIST) – the body, as directed under HAVA, that will conduct an evaluation of independent, non-federal laboratories to conduct testing, certification, de-certification, and re-certification of voting systems.

Object Code – the version of a computer program in the machine language of the computer on which it is to be used.

Operation Manual – a manual of all procedures used to prepare, operate and maintain the voting equipment, including the unpacking and storage procedures to be used by local elections officials.

Parallel Monitoring (also known as 'random on-site sampling' or 'Election Day

sampling') – a testing procedure in which voting machines are randomly taken out of service on Election Day and are voted on by State testers in order to simulate a true election and determine if the votes cast are correctly recorded. The testers would vote according to a prepared script in order to detect if the software is recording votes correctly.

Qualification Testing - testing at the national level by an ITA against the FEC's Federal Voting System Standards. Successful completion will place a vendor's product on a list of "Qualified" voting systems, meaning that they have been tested and found to meet or exceed the standards specified in the FVSS. Vote tabulation software, including source code, and election management software will be examined by a NASED approved ITA. The software ITA will handle any software that tabulates or reports votes and vote totals and which is not in a permanent machine resident status (on a ROM). This includes software that is resident on a computer hard drive or any software that is external to the voting system.

Software – the application and operating system programs associated with a computer or voting device, as opposed to hardware that refers to the physical components of a computer system. The term "software" includes any and all codes for operation of the vote counting system including ballot tabulation system bootstrap, monitor and device controllers, operating system, ballot layout, system audit, and report generation.

Source Code – the specific language a programmer uses to program the electronic equipment or vote tabulating system.

Test Deck – a pre-audited group of ballots voted with a pre-determined number of votes.

Vendor – any manufacturer, company, or individual who seeks to sell, or sells, a voting system or a vote tabulating system for use in California elections.

Voter Verified Paper Audit Trail (VVPAT) – a paper representation of a voter's choices that is verified by the voter at the time he or she casts his or her ballot.

Technical Oversight Committee – a committee proposed by the Ad Hoc Touch Screen Task Force that should be comprised of technical experts who can improve current testing standards, provide expert guidance throughout the certification process, and serve as a panel to review software and hardware issues that might arise.

Vote Tabulating Device – any piece of equipment, other than a voting machine, that compiles a total of votes cast by means of ballot card sorting, ballot card reading or scanning, paper ballot scanning, electronic data processing, or a combination of such equipment.

Vote Tabulating Program – the computer programs used for counting of votes cast on Ballots. It includes any and all vendor software, and the coding programs specific to each election.

Voting System – any mechanical, electro-mechanical, or electronic system and its software, or any combination of such, used to cast or to tabulate votes, or both.

Voting System Procedures – detailed procedures for operating a voting system adopted by the Voting Systems and Procedures Panel when a system is certified and available to the public.

SUBMITTAL

The undersigned members of the Ad Hoc Touch Screen Task Force hereby submit this Report to Secretary of State Kevin Shelley for his consideration:

/s/
Mark Kyle, Chair

/s/
Marc Carrel, Co-Chair

/s/
Kim Alexander

/s/
David Dill

/s/
David Jefferson

/s/
Robert Naegele

/s/
Shawn Casey O'Brien

/s/
Mischelle Townsend

/s/
Charlie Wallis

/s/
Jim Wisley