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.