March 2, 2004
Statewide Election Report

Prepared by the Office of the Secretary of State

April 20, 2004

KEVIN SHELLEY | CALIFORNIA SECRETARY OF STATE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

An election is an exercise in democracy — an opportunity for Americans to express the "consent of the governed." At the same time, it is an enormous and complicated logistical undertaking, requiring the organization and integration of both people and machines to ensure that the election produces accurate and secure results. Moreover, voters must have complete confidence that their votes are correctly counted.

On the front lines are county elections officials and pollworkers who take charge of the many tasks critical to conducting a statewide election. Working with the Secretary of State, county election officials are charged with implementing the laws designed to ensure that elections are conducted fairly and efficiently. Californians are truly indebted to these officials and pollworkers whose dedication, hard work and commitment to public service are to be commended.

The main focus of this report is to identify problems that were experienced at the March 2 Primary Election and propose solutions to prevent those problems from recurring in future elections.

We are in a time of change. Prior to the presidential election in 2000, the administration of elections received little attention from the public or the media. As a result of the problems that occurred in Florida in the November 2000 election, however, the "infrastructure of democracy" has been the subject of intense focus and public scrutiny – particularly the equipment that is used to cast and count ballots.

The equipment we use to vote and to count ballots must meet the needs of elections administrators, but, more importantly, *it must meet the needs of the voters*. As we move to new, and more modern voting technology, we need to recognize the advantages of this technology. But the fact that technology is new does not automatically mean that it is better. As with any new technology, it must be continuously scrutinized and improved. And, we must ensure that the people operating the machines are well trained in the use of that new technology to further ensure that the elections are run in a fair and orderly manner. Finally, we must take the steps necessary to assure voters that when they cast their ballots on new electronic equipment, the machines they vote on will accurately record their vote, and the county tabulation system will accurately count all votes cast.

One of the biggest challenges facing elections officials is how to manage the transition to new technology and to ensure that the cornerstone of our democracy remains accurate, convenient and secure. Again, the experience in Florida – this time in its September 2002 primary election – is instructive. In response to the problems with the

now-infamous prescored punchcard voting systems, the State of Florida rushed to implement electronic voting, which resulted in yet another flawed election. (See *Voting problems in Florida? Count on It: Glitches plague primary despite millions spent on improvements* (San Francisco Chronicle 9/11/2002).)

In response to numerous reports of difficulties throughout the state, the staff of the California Secretary of State conducted a comprehensive review of the performance of electronic voting devices (commonly referred to as "DREs" or "touch screens") used in the March 2, 2004 Statewide Primary Election (March Primary). This review was particularly critical because the March Primary was the first election in which a large percentage of registered voters (43%, or almost 6.5 million voters) were able to use these devices on Election Day.

Touch screen systems are a promising technology for a number of reasons. Touch screens can prevent voters from invalidating their votes by voting for more candidates than permitted for a particular office, allow for many languages to be conveniently displayed, and are accessible for members of the disability community.

However, in the period before, during and after the March Primary, numerous problems and concerns have emerged. These problems and concerns suggest that DRE technology may not yet be stable, reliable and secure enough to use in the absence of an accessible, voter-verified, paper audit trail (AVVPAT). Presently, many election systems allow counties to print out hard copies of votes from their election systems at the end of election day voting. Unfortunately, because voters have no opportunity to verify these records at the time of voting, the records are nothing more than a paper copy of the data on the machine. If the data is corrupted or has been altered, the paper copies will merely reflect electronic tabulation of that corrupted or altered data.

A voter verified paper trail, on the other hand, allows voters to verify that their vote has been correctly recorded on paper at the time it is cast. Because that paper record has been verified by the voter, it provides the basis for conducting a meaningful manual recount. And an AVVPAT provides voters confidence that their electronic vote has been accurately recorded. Although most election vendors are developing AVVPATs, it is unclear whether those systems will be federally approved, manufactured and deployed in time for the November election.

The difficulties experienced surrounding the March Primary fall roughly into five categories:

1. Pre-election issues including equipment and software testing, certification and qualification issues;
2. Reliability issues;
3. Security issues;
4. Accuracy issues;
5. Training issues.

Pre-election Issues:

In the 60 days prior to the election, every manufacturer of DRE equipment used in the March Primary sought approval of last-minute changes to software, firmware and hardware. In some cases, these were minor modifications caused by changes in state laws regarding eligibility of independent (decline to state party affiliation, or DTS) voters to participate in party primary elections. In other cases, however, these changes involved completely new pieces of equipment or revisions in software and firmware. The latter proposed changes were particularly troubling since many of them had not received federal qualification – and, in some cases, had not even been tested for such qualification. Especially troubling was the fact that many vendors and registrars asserted that, without the requested uncertified and untested changes, the election could not be conducted successfully.

The process of approving election software and hardware is evolving. Historically, most testing of election equipment has been focused on functional testing of the mechanical aspects of voting systems – to determine whether the equipment functions as needed in recording and tabulating votes. The advent of computerized equipment has required a fundamental change in testing procedures because software must be analyzed for "bugs," "malicious code," "back doors" and similar security problems that could result in errors or could create the potential for tampering. Often, these problems will not be detected by functional testing.

Our state certification procedures require federal qualification of equipment and software prior to state certification. This federal qualification involves testing by independent testing authorities (ITAs) approved by the federal government. The Help America Vote Act of 2002 (HAVA) transferred the responsibility for overseeing the federal qualification process from the Federal Election Commission to a newly created entity, the Election Assistance Commission (EAC), which only recently held its first meeting. Similarly, HAVA transferred the responsibility for adopting federal voting system testing standards from the National Association of State Election Directors

(NASED) to the National Institute of Standards and Technology (NIST). These transfers in authority have led to delays in receiving federal qualification.

The State's own certification process requires vendors to notify the Secretary of State of proposed changes to voting systems. State procedures also require that changes to hardware and software be approved by the Secretary of State, based on public hearings and recommendations by the Voting Systems and Procedures Panel (VSP), which meets on 30 days notice. State testing and preparation of staff reports must occur before the panel meets. Many of the requests that have been submitted by vendors for changes to their voting systems with respect to the March Primary Election completely ignored this process.

Vendors' very late submission of proposed software and hardware changes is one indication that electronic voting technology is still evolving. While that evolution is generally positive – and typical of computer systems development globally – *elections systems must be more stable, secure and reliable than computers used in homes and offices*. Election day voting captures a single moment in time; if the results of the election are lost or corrupted by outside tampering with the voting system, there may be no way accurately to recreate the event or to breathe legitimacy into the result.

This problem is especially acute with touch screens. Because touch screens presently lack an accessible, paper audit trail that voters can independently verify at the time they cast their electronic ballots, there is no reliable means to reconstruct the election if the electronic record of the votes is subject to question. Even a paper printout of ballots by the touch screens at the end of the election day will not provide confidence to the voters that their votes have been accurately recorded *unless the voters verified those ballots at the time the voters cast them*.

Finally, given that vendors continued to request changes to voting systems *after* the March Primary to address problems with touch screens used in that election, there is every indication that the disturbing pattern of last-minute requests to approve modifications to touch screen systems will continue during the preparation for the November 2004 election.

Reliability Issues:

Much of the public discussion regarding problems with the March Primary focused on reliability problems experienced with DREs. Very significant reliability issues arose in both San Diego and Alameda Counties – both of which use systems produced by Diebold Election Systems, Inc. (Diebold). The difficulties were mostly attributable to a device referred to as a "PCM," (Precinct Control Module) which is used to create

cards that voters use in order to gain access to the touch screen voting machine. The information encoded on the card tells the touch screen machine the ballot type to display. The Secretary of State's Office denied Diebold's request for certification of the PCM machine because Diebold had failed to obtain the federal qualification for the device. Just weeks before the election, however, a number of county registrars felt compelled to challenge this ruling, asserting that the impending election could not be conducted without the equipment. Because Diebold had only secured limited functional testing of the PCM device, the Secretary of State's Office administratively approved the PCM device for use only in the March Primary.

Secretary of State testing of the PCM devices suggests that the primary cause of the problems reported on Election Day was that the device's battery continued to drain even when the unit was in the "off" position. Diebold neither alerted elections officials about this problem, nor did it indicate to counties that additional pollworker training or documentation was necessary to address this problem. Diebold's own investigation report concedes that its equipment created the problem, not pollworker error.

The net effect is that the problems with the PCM device, together with a lack of documentation and training by the vendor about how to resolve the problem, led to a "worst case scenario" in San Diego County, and serious difficulties in Alameda County. Most polling places had only one PCM machine. Therefore, when the device failed, there was no means for voters to access and use the touch screen machines in that polling place.

Without access to the touch screens, voters could not vote. This is because San Diego County, despite repeated recommendations from this office, failed to provide back-up paper ballots at polling places. As a result, over half of San Diego's polling places could not open on time as a result of the PCM failure and the failure to provide back-up paper ballots. Voters were turned away or sent to other polling places to vote provisionally. Presumably, some of these voters cast their ballots later in the day. **There is no way to estimate the number of voters who failed to return to the polls after being turned away.**

In Alameda County, back-up paper ballots were available at the polling places. Accordingly, most voters were able to cast provisional ballots that were ultimately counted.

Security Concerns:

During the past year, four formal studies of electronic voting systems have been published by a broad range of security experts. These reports are commonly referred

to as the Hopkins Report (by Tadyoshi Kohno, Aviel Rubin, Adam Stubblefield and Dan Wallach), the SAIC Report (commissioned by the State of Maryland), the Compuware Report (commissioned by the Ohio Secretary of State), and the RABA Report (commissioned by the Maryland Department of Legislative Services.)

These studies have all exposed serious security problems with touch screen systems. These reports have made numerous recommendations for changes, both in the short term and long term. Some of the reports concluded that, even with changes, some form of paper audit trail will be necessary to ensure the security of these systems.

In response to these reports, the Secretary of State issued a series of security directives and advisories to county election officials. Despite these directives, the security measures taken by manufacturers and some counties were inadequate. Although some manufacturers have begun to address security concerns in their hardware and software, many of these efforts came too late to achieve federal qualification and state certification for the March Primary. The likelihood that needed changes will be made, tested and federally approved for the November election is diminishing.

In short, while no significant security breaches were detected in connection with the March Primary, security issues have not been adequately addressed. Addressing these issues is of critical importance both to ensure that future elections are secure, and to ensure that voters have confidence their votes will be recorded and counted correctly.

Accuracy Concerns:

It is impossible to gauge the accuracy of the touch screen machines effectively in the absence of an accessible, voter-verified paper trail. However, to the extent that accuracy can be assessed, it is clear that touch screen voting systems experienced accuracy problems at the March Primary. These problems were not attributable to the touch screen machines themselves, but to the interaction between the machines and pollworkers. The bulk of these accuracy problems involved pollworkers who were unfamiliar with computer technology. In many instances, the pollworkers encoded access cards improperly, resulting in voters receiving and often using the wrong electronic ballot type.

Training Issues:

The March Primary revealed a central shortcoming of high technology voting equipment: When things go wrong, often only those with experience and knowledge of computer systems can fix them. As a result, media accounts of the March Primary are full of stories about teenagers “rebooting” election machines that had stumped poll

workers. While these accounts may be humorous to some, only authorized election officials should have access to the inner workings of voting machines on election day. It also highlights a critical problem with touch screen systems: many poll workers are not technologically sophisticated. This problem is exacerbated by the fact that in many cases manufacturers have failed to provide adequate documentation and training to elections staff, and that many of the error messages generated by the machines provide no information about how to fix the problem.

Training problems were manifested in a number of ways at the March Primary. In Orange County, a DRE county, pollworkers provided many voters with incorrect electronic ballots because voters from a number of precincts voted in the same polling place and pollworkers erred in assigning voters the correct ballot type. This problem was a mixture of the complexity of the technology and training issues.

The Diebold PCM problem also revealed a training problem because poll workers had not been provided adequate information to bring the system online after its startup problems. In many cases, reviving the PCM machines was only a matter of a few keystrokes, but no one had trained poll workers to perform this task. And, again, the machine itself provided error messages that few were trained to interpret.

This problem can and must be addressed – but the "fix" is neither simple nor easy. Until computerized elections systems become far more stable and user-friendly, poll workers will need to be far more tech-savvy. This will require additional training, as well as recruiting more qualified poll workers.

Moreover, an underlying problem – which will not change between now and the November 2004 election – is that touch screen systems are continuing to evolve. New components are being added, and the systems are constantly being modified. New problems inevitably will accompany those changes. As the PCM problem demonstrates, potential problems may not be discovered until election day. Accordingly, there is a significant risk that new problems will arise at polling places at the November 2004 election, and given the technological complexity of touch screen voting systems, most poll workers will be no better able to resolve those problems than they were with the PCM problem encountered at the March Primary.

Conclusion:

Many of the difficulties encountered with touch screens at the March Primary can be addressed. The technology exists to build reliable, secure systems with accessible, voter-verified, paper trails. It is unclear, however, whether the issues identified in this report either can or will be addressed adequately in time for the November election.

This concern is based on the following:

- Much of the touch screen software and firmware currently in use, particularly Diebold equipment, is certified on only a one-time or conditional basis – if at all. Very little of the touch screen equipment has a federal NASED approval, and none has qualified under the new 2002 standards. Given this failure by touch screen vendors to obtain necessary testing and approval, and the delays in the federal approval process because of the transfer of testing and approval authority from the Federal Elections Commission to the Election Assistance Commission, it appears unlikely that touch screen systems will be fully tested and approved prior to the November 2004 election.

- Much of the equipment in use has significant reliability issues that will require continuing software and hardware modifications which have yet even to be proposed. Moreover, touch screen vendors have provided no indication that, in the next six months, they will be able to resolve the systemic problems that led to numerous last-minute requests for modifications to their touch screen systems.

- The technological sophistication of touch screen systems, along with their continuing evolution, and their user-unfriendliness, pose a continuing challenge for election workers who will require extensive training for the problems that have been identified, and who will be largely unable to address problems that arise for the first time at the November 2004 election.

- Changes in both the federal qualification and state certification processes are needed. At the federal level, systems must be implemented to expedite the testing and approval of equipment. At the state level, if the problems addressed in this report teach us anything, it is that the Secretary of State's office should not, in the future, allow the use of equipment or software without full federal testing and qualification, source code review, and review by the Secretary of State's Voter Systems and Procedures Panel (VSP) whenever a significant change is made. The Secretary of State's Office shares responsibility for some of the problems that occurred at the March Primary because it should not have authorized the last-minute changes requested by vendors, when those changes had not been adequately tested, and had not received federal approval.

- A great deal must be done to address the security concerns identified in a number of reports by respected computer experts. These security issues are very real. More troubling, however, is that we do not yet know all of the security

vulnerabilities of computerized election machines. Is it possible someone might want to hack or disrupt electronic voting? Given the history of computers and the internet, this concern is not purely speculative. Without an AVVPAT, it is entirely possible that votes could be lost in a manner that cannot be reconstructed.

An accessible voter-verified paper trail would provide an important level of protection against known and unknown security issues, and provide the public with confidence that their votes are being counted accurately. Some vendors are developing such systems, but the critical question is whether those vendors will be able to get federal qualification and state certification in time to produce those systems in sufficient quantity to be used in the November election.

INTRODUCTION

California's March 2, 2004 Primary Election was notable for several reasons. It set a record for the percentage voters who voted using absentee ballots -- nearly 33%. It was the first election in recent times in which no pre-scored punch card voting machines were used. And finally, it was the first election in which over 40% of the voters could vote on electronic voting systems on Election Day.

The way in which Californians are voting is changing profoundly. Overall, these changes are positive. The passage of both the state's Shelley-Hertzberg Voting Modernization Bond Act of 2002 (Proposition 41) and the federal Help America Vote Act of 2002 (HAVA) have provided the funds necessary to eliminate the now-infamous prescored punch card voting systems that made "chad" a household word. There are now three types of voting systems being used in California. A small number of counties continue to use non-prescored punchcard systems that do not produce the "chad" problems that plagued the 2000 election. Many counties now use an optical scan system. With this system, voters fill in spaces provided on ballots that are then read by a scanner. Finally, many counties have purchased direct recording electronic (DRE) systems, which are commonly referred to as "touch screens." With touch screen systems, voters record their votes by touching or moving a cursor on a computer screen, recording their vote selections on memory cards and hard drives.

Electronic voting on DREs is easier and more accessible to disabled voters and those whose primary language is not English.[1] For this reason, HAVA requires that every polling place include at least one DRE by 2006. There is also evidence that DREs reduce under-voting and eliminate over-voting – a frequent cause of punchcard ballots being discarded.

However, the events leading up to, during and immediately following the March Primary also revealed the many unresolved challenges we face on the way to implementing electronic voting successfully.

[1] Electronic voting systems are touted and promoted for their ability to provide increased access to the disabled and those whose primary language is not English. It remains a concern whether the technical tests received at the federal level, particularly under the 1990 federal standard, but even under the 2002 standards, are an adequate substitute for real-world testing by individuals whose voting access is limited. Assuring the privacy and independence of disabled and non-English speaking voters during the voting process is critical to assuring that every voter can cast a secret ballot. For systems that have met the technical requirements of accessibility under the federal standards and can be used by those with disabilities, meeting minimum requirements does not ensure that they are easy to use, intuitively designed, or functionally comfortable for disabled or non-English speaking voters.

These challenges include the security of touch screen systems, their reliability and accuracy, as well as the adequacy of pollworker training. Resolving these problems is especially critical because, currently, there is no voter-verified paper trail or other device that would enable election officials to reconstruct voter intent in an election if the data recorded on a machine is corrupted or the software is faulty. Printing a paper record of votes or images of the electronic ballots at the end of the day is not an effective substitute for a voter verified paper trail. Unless the voter has verified at the time he or she votes that the paper record accurately reflects the votes cast, the content of the paper record is just as subject to manipulation as the electronic tally.

Although the Secretary of State has previously directed that a voter-verified paper trail accessible to disabled voters will be required for new systems by 2005, and all systems by 2006, it is unclear at this time whether vendors will be able to produce such systems, obtain required federal and state approval, and install them in time for the November presidential election this fall. (See **Appendix I** – Position Paper and Directives of Secretary of State Kevin Shelley Regarding the Deployment of DRE Voting Systems in California).

Given these concerns, the Secretary of State's Office has conducted a comprehensive review of the administration of the March 2, 2004 Statewide Primary Election, with a focus on the widespread use of DREs. This is the first time such an extensive review has been conducted and the results reported.

ASSESSMENT AND ANALYSIS

The following is a summary and analysis of the most visible problems reported on Election Day. More detailed reports on methodology, as well as various aspects of the problems experienced with respect to touch screen voting equipment, are attached as exhibits to this report.

There are five key areas in which difficulties were encountered:

1. **Pre-election Issues** – Compliance by voting systems vendors with the legal, regulatory, and procedural requirements necessary for a system to be eligible for use in California elections.
2. **Reliability** – The sturdiness and dependability of the systems.
3. **Accuracy** – The confidence that the systems are tabulating votes correctly.
4. **Security** – The assurance that the systems are fortified from tampering and there are no weaknesses that can be exploited.
5. **Training** – The assurance that pollworkers have received adequate training before election day to enable them to properly operate and resolve problems that develop with touch screen systems at the polling place.

We analyze the problems faced at the March Primary in each of these five categories.

I. PRE-ELECTION ISSUES

Before voting systems may be used in California elections, they are tested and approved under federal standards, and then certified by the Secretary of State under state standards. Similarly, voting system vendors are required to notify the Secretary of State before making any modifications to voting systems or components so that such modifications can be tested and approved before the modified system or component is used in a California election. Because it can often take months for testing to be completed at both the federal and state levels, it is incumbent upon election system vendors to submit their systems for testing well in advance of any election at which those systems are intended to be used.

On numerous occasions in the days and weeks leading up to the March Primary, DRE vendors failed to timely seek federal qualification and state certification of voting system components intended for use in that election. Vendors often submitted proposed modifications to voting systems for state review and testing without having them first reviewed, tested and qualified under federal standards. Then, having failed

to obtain approval at the federal level, vendors and counties urged the Secretary of State to expedite testing of software or hardware immediately so it could be used in the March Primary. Frequently, counties and DRE vendors had no backup plan in place if last minute applications failed testing. The result was a choice between using equipment that had not been fully tested and approved, or using no equipment at all.

A. The Federal and State Approval Process.

Federal testing, performed by federally authorized independent testing authorities (ITAs), consists of functionality tests of the system's software, hardware and firmware to ensure that the system will perform as intended, and will comply with federal requirements for conducting elections. A line-by-line source code analysis is included in this testing regimen. Federal testing also includes tests to determine the ability of a machine or system to withstand environmental and physical stress.

The Secretary of State then examines system functionality further to evaluate its ability to comply with state requirements. This testing examines the system's ability to accurately conduct a statutorily-required one-percent manual recount, its ability to rotate candidates as required by California, and its ability to allow decline to state voters to vote for some or all partisan offices and other California-specific requirements.

The 1990 federal Voting System Standards used by ITAs were revised and strengthened in 2002, but very few systems have been tested under the 2002 standards. Once a system completes testing and has met all of the requirements of the federal standards, the system receives a federal qualification number pursuant to standards adopted by the National Association of State Election Directors (NASED). The system is then eligible to be considered for certification by the Secretary of State. Once a system has completed all of the state tests and has been determined to have met all of the state requirements, the system may be certified by the Secretary of State.

B. Failure of Voting System Vendors to Timely Seek Federal Qualification and State Certification for Components Intended for Use in the March 2004 Election

In the weeks immediately prior to the March Primary, numerous applications for certification were submitted by the four vendors whose DRE systems were used on March 2nd, as well as by Los Angeles County, which runs a unique system they have developed that incorporates aspects of Diebold equipment. The Secretary of State's Office received ten requests in the eight weeks before the election from Diebold Election Systems alone. In addition, there were three requests from Elections Systems & Software (ES&S) and one request each from Hart InterCivic, Sequoia, and Los

Angeles County. Where the vendor was applying for a federally qualified device or software change supported by the documentation necessary to allow us to conduct a proper evaluation, the Secretary of State's Office acted expeditiously on the application.

The Sequoia application was submitted on January 2, 2004 prior to receiving federal review. The application sought approval for a modification, which involved an export of data in a more efficient and manageable manner for the counties. This modification was in response to conditions that we had placed on a previous certification. Since the Sequoia software change was still undergoing federal testing, the vendor utilized a work-around method with their existing certified software.

Los Angeles County made a request on January 9, 2004 for a change in their software to permit the reporting of Decline to State (DTS) voters who choose to vote in certain party primaries, as allowed by a 2003 change in state law. The Los Angeles request was tested and administratively approved for use on February 11, 2004.

Hart InterCivic submitted an application on January 1, 2004 for approval of a minor modification to its absentee voting equipment. The modification would move the bar code on absentee ballots so they could be mechanically scanned for sorting and mailing of absentee ballots. The application had been federal reviewed prior to being submitted to this agency, and after state testing and receipt of the federal NASED qualification number, it was also administratively approved for use on February 11.

ES&S submitted three applications on February 2, 2004 just one month before the election. One application was for modifications to its precinct optical scan unit, one application was for its central count optical scan unit and one application was for modifications to its central count systems, all of which were designed to accommodate the DTS ballots. ES&S withdrew two of their requests after work-arounds were completed. ES&S indicated that one of their requests was simply a notification since they planned to revert to a previous version of software. But when informed by staff that the version of the software they sought to use had never been certified for use in California, ES&S rescinded its applications and developed a work-around process.

Diebold submitted a total of ten applications for approval of new or modified devices and software during the eight weeks prior to the March Primary. Six of these applications were rejected since the devices and software had either never been federally tested or had not been federally qualified. Many of the proposed modifications had not received federal qualification, or even been tested under federal standards.

Diebold did, however, submit some applications that were tested and conditionally approved for use on a one-time only basis for the March Primary. The first application was a software patch for Alameda County to process paper absentee and provisional ballots. This patch was intended to correct a problem that was caused by uploading more data into the barcode field than the Diebold system was able to properly process. As a result, optical scan devices were unable to completely read the data. Similarly, this agency conditionally approved a software patch to allow data from Diebold TS DRE units used during early voting to be exported into a particular file format for inclusion into Los Angeles County's InkaVote tabulation system. This was conditionally approved on February 26, 2004 for one-time use in the March Primary.

Early in February 2004, Diebold sought approval to the firmware used on its TSx touch screen system. Despite the misgivings about its late application, this modification was granted conditional approval for use in the March Primary.

The final application from Diebold seeking approval of equipment in the weeks before the election concerned the PCM 100 and PCM 500 card encoding devices. Diebold initially delayed in demonstrating these devices to Secretary of State staff, and in submitting the necessary documentation regarding PCM devices.

The Secretary of State's Office received Diebold's documentation on January 8, 2004, and after reviewing the request, informed Diebold that it would need to obtain either federal review, or a waiver letter from an ITA indicating that no federal testing was required. After consulting with Wyle Laboratories, the federal ITA that reviewed the devices, Diebold was told it would need to seek a formal review of the devices.

On February 2-3, 2004, Secretary of State staff agreed to review the devices in McKinney, Texas with other Diebold items they were testing. Diebold, however, had still not submitted the items for federal review and was told by the Secretary's technical staff that given the late date, Diebold should ensure that it had a back-up method using fully certified equipment for each of its clients that needed to encode smart codes for Diebold DRE machines.

On February 13, 2004, the Secretary of State's Office notified Diebold by letter that as a result of the lack of a federal testing report, its PCM devices could not be used in the March Primary.

As a result of this letter to Diebold, the registrars of voters of the two largest counties using Diebold DRE systems contacted the Secretary of State's Office. On February 17, 2004, in a telephone conference call between the San Diego Registrar of Voters and several members of the Secretary of State's Elections Division staff, the Registrar

indicated that San Diego election officials had no choice but to use the PCM devices for the March Primary - with or without state certification. Secretary of State staff suggested an alternate method be used, but the Registrar found the suggested alternatives unacceptable.

A day earlier, the Alameda County Registrar sent an email to the Secretary's Election Division Chief stating, "I was just informed of your late Friday letter to Diebold regarding the card encoder. I will be unable to conduct the primary election on March 2 without this equipment. I believe that your office could provide a conditional administrative approval of these card encoders. Without this cooperation there will be thousands of people unable to vote. This situation is intolerable and well within your office's ability to solve."

Several days later, due to time constraints, Wyle Laboratories deferred testing to Ciber, another federal ITA, and Ciber tested the devices. A report from Ciber arrived at the Secretary of State's Office on February 20, 2004 approving limited use of the PCM devices for the March Primary only. Based on this letter of conditional use by a federal ITA, the Secretary of State's certification and technical expert reviewed the device and also recommended limited approval of the devices for use in the March Primary. Accordingly, on February 23, 2004, the Secretary of State's Office administratively approved the PCM devices for limited one-time only use.

Taken as a whole, the numerous requests for last-minute approval of voting system components for the March Primary highlights a significant problem with the certification process. Under this process, vendors and registrars are requesting review of voting systems and software at a moment's notice, often just days before an election, and expect state approval regardless of the status of federal testing.

This approach to system certification must change. Voting system vendors can no longer be allowed to submit applications for approval at the last minute, often without having first obtained federal qualification of the proposed modification, and expect the Secretary of State's Office to consider those applications. We share responsibility for this problem by failing to set a firm deadline beyond which no further applications would be considered. Rushing the testing process creates the chance that the tests will not be complete, and only encourages more last minute applications. Accordingly, by no later than June 1, 2004, the Secretary of State should establish such deadlines for the November 2004 election.

Finally, and significantly, the number of inexcusably late requests for voting system modifications by touch screen vendors strongly suggests that this computer technology is very much still a work in progress. Outside of elections, the fact that a computer

system is evolving and in need of constant change might prove inconvenient for an individual computer user, and costly to a business. In the context of an election, where voters exercise their constitutional right to democratically choose their elected representatives, this process is not acceptable.

II. RELIABILITY

Reliability of a voting system is critical because failure of a voting system before or during the voting process may cause delays, and, in extreme cases, may prevent voters from casting their ballots. If a system fails during the central tabulation process, this failure can result in votes being miscounted.

The reliability of the voting systems was an issue at the March Primary in San Diego, Alameda and Napa Counties. San Diego and Alameda both experienced problems with Diebold's PCM-500 devices, resulting in the inability of many voters to cast ballots. Napa County experienced problems with its Sequoia vote tabulation equipment.

A. San Diego County

Of a total of 1,038 polling places in San Diego County, 573 (55%) were unable to open on time on Election Day. A significant percentage of polling places opened at least one hour late. The reason for this was that the Precinct Control Module (PCM-500) that was used with the Diebold AccuVote TSx voting system, which encodes voter access cards with the code for the voter's proper ballot type (and thus enables voters to use touch screen machines), did not function properly. This problem represented a "single point of failure" for the entire voting system, because the PCM device controls voter access to all touch screen units at a polling place.

Secretary of State testing of the PCM devices concluded that the primary cause of the problems reported at the March Primary was that the battery continued to drain even when the PCM device was in the "off" position. When the battery was completed drained, poorly written computer code resulted in the devices displaying a window unfamiliar to poll workers.

Moreover, Diebold neither alerted elections officials about this problem, nor did it indicate to counties that additional pollworker training or documentation was necessary to address this problem. Indeed, Diebold's own investigation report concedes that its equipment created the problem, not pollworker error.

This was compounded by San Diego County's decision to not provide paper ballots at the polling places as a back up, as requested by the Secretary of State's Office, and to utilize electronic provisional ballots rather than paper provisional ballots. As a result, an unknown number of voters who arrived at the polls in the morning were unable to cast ballots. Most voters were directed to either go to nearby polling places to vote an electronic provisional ballot or to return later in the day after the equipment problem was resolved. These voters either voted provisionally or returned to vote later.

Critically, though, there has been no reliable estimate of the number of voters who were turned away and *were never able to cast a ballot at all*. These voters were completely disenfranchised.

In addition, San Diego County indicated that it had discovered an error in the Diebold software that tallied absentee ballots. The error was discovered after the county certified the results. The county had to re-tabulate its absentee ballots and submit an amended election certification. According to the county, approximately 3,000 votes were at issue in the presidential primary, but neither the outcome of that contest nor any other contest was affected.

B. Alameda County

Alameda County, which used the Diebold AccuVote TS system (a precursor of the AccuVote TSx model), experienced the same problem with the Diebold PCM device experienced by San Diego.

To Alameda's credit, because it had paper provisional ballots available at the polling place, voters who arrived at their polling places before the county fixed the PCM problem were able to vote with paper provisional ballots. In a few instances, however, polling places ran out of provisional ballots before the PCM devices were fixed. This resulted in the potential for some voters not being able to cast a ballot.

In addition to the failure of the PCM device during the process of opening the polls on Election Day, Alameda County also had several of these devices fail during the day, highlighting a significant reliability issue with the devices. The reasons for the failure of the PCM-500 used in San Diego and Alameda Counties is explained more fully in the PCM Report. (See **Appendix II – PCM Report**).

C. Napa County

In Napa County, Sequoia's AVC Edge DRE system experienced several equipment problems including frozen screens. In addition, Napa County's 400-C optical scan ballot vote tabulation equipment failed to register marks made by dye-based ink on a significant number of vote-by-mail ballots. This was discovered during the statutorily required 1% manual recount of ballots counted by machine. The vote-counting equipment was found to have been calibrated incorrectly during election set-up and 13,300 vote-by-mail ballots needed to be reprocessed.

D. Plumas County

Plumas reported a problem that occurred six times throughout the county, in which an error message was displayed when a voter tried to write-in two or more candidate names on certain types of electronic ballots. These six voters were allowed to vote a paper ballot.

E. Kern County

Kern County reported minor equipment problems with the PCM 100 devices and with printers on the TSx. Because of software inadequacies, the county also faced problems processing provisional ballots of some DTS voters cast in incorrect precincts. This same problem also occurred in San Diego and San Joaquin counties.

F. Solano County

Solano County experienced mostly minor problems consisting of a few frozen DRE screens.

Solano County avoided the PCM problem experienced in Alameda and San Diego counties by early detection of the low battery charge problem. Based on this discovery, pollworkers were directed to ensure that the PCM devices were charged over the weekend prior to the election so that they would be fully charged on Election Day.

III. ACCURACY

The accuracy of an election is tied directly to the individuals and machines used to record and count the votes. If a system fails to record votes accurately or to tabulate

votes correctly, this leads to skepticism about the system used, and indeed the entire election process. The result is that the confidence of the electorate is undermined.

Needless to say, accuracy is also directly dependent upon each voter being given the correct ballot. If a voter is not provided the ballot corresponding to the voter's residence, he or she will vote on the wrong ballot.

Issues of accuracy arose in several counties during the March Primary. San Diego County experienced problems with software counting votes, while Orange and Napa Counties provided incorrect ballots to voters.

A. San Diego County

The tabulation software in San Diego County did not properly process provisional ballots voted in accordance with Elections Code section 14310(c)(3)(B). In September 2003, the Legislature enacted a statute that allows a voter to vote provisionally in any precinct in his or her county. The tabulation software was not capable of implementing this change in the law. Although the law was changed in 2003 and Diebold discovered this problem during pre-election testing, Diebold did not request approval of a software change until March 19, 2004 — nearly 2 ½ weeks *after* the election, and only 11 days before the county was required to certify the official results of the election.

Moreover, the software for which Diebold sought last minute approval had not been presented to a federal Independent Testing Authority (ITA) for testing, and accordingly had not been federally qualified for use. Nor had it ever been submitted to the state for testing and certification. Ultimately, Diebold withdrew its late request for approval and was required to devise an alternate method for tabulating provisional ballots.

Also, as previously noted, San Diego County discovered an error in the Diebold software that tallied absentee ballots, which required the county to re-tabulate its absentee ballots and submit an amended election certification.

B. Orange County

In Orange County, some voters received incorrect ballots at the polling place. In some instances, where a single polling place was used for a number of precincts with different ballot types, pollworkers were required to be extremely careful using the voting equipment in order to provide voters with the appropriate ballot

code. When a pollworker selected incorrectly, the voter could receive the wrong ballot.

One source of this error was inadequate pollworker training. The problem was compounded by a design problem in the Hart DRE voting system.

C. Napa County

In Napa County, officials erred in mailing incorrect ballots to up to 90 persons who were registered as "permanent absentee voters." This was a human error, and in the end the number of potentially incorrect votes was not enough to affect then outcome of any contests.

Paper ballots were the key to assessing performance. Where they were available, paper ballots confirmed that incorrect ballots were provided to voters, and they confirmed that the tabulation of absentee ballots was incorrect. Where paper ballots were not available, it was impossible to determine whether other accuracy issues arose related to the electronic recording and tabulating of votes.

Finally, while California law requires a one percent mandatory manual recount, in the absence of an accessible voter verified paper trail, such recount procedures are of little value for DRE systems. The purpose of this manual recount process is to detect problems with the operation of the touch screens and tabulation systems. However, where the voter is unable to verify at the time he or she votes that the paper record accurately reflects his or her selections, the paper record provides little, if any, assistance in determining whether the electronic voting and tabulation systems properly recorded and counted his or her vote.

IV. SECURITY

A. Published Security Studies on Electronic Voting Systems

In the last year, there have been at least four nationally recognized studies of electronic voting systems published by security experts. These studies have all exposed significant security issues with these systems, and made numerous recommendations for major changes.

The reports we reviewed are the following:

- The Hopkins Report, formally titled "Analysis of an Electronic Voting System", by Tadyoshi Kohno, Aviel Rubin, Adam Stubblefield and Dan Wallach, IEEE Symposium on Security and Privacy, 2004, IEEE Computer Society Press, 2004.

(Originally published in July, 2003; also available at www.avirubin.com/vote.pdf)

- The SAIC Report commissioned by the State of Maryland entitled "Risk Assessment Report Diebold AccuVote-TS Voting System and Processes", (published only in heavily redacted form in September, 2003 and available at www.dbm.maryland.gov/DBM%20Taxonomy/Technology/Policies%20&%20Publications/State%20Voting%20System%20Report/stateVotingSystemReport.html)
- The Compuware Report, commissioned by the Ohio Secretary of State, entitled "Direct Recording Electronic (DRE) Technical Security Assessment Report". This report was published in November, 2003, and is available at http://www.voterwest.org/ohio-compuware-study.pdf
- The RABA Report, entitled "Trusted Agent Report Diebold Accuvote-TS Voting System," commissioned by the Maryland Department of Legislative Services and published in January 2004. It is available online at http://www.raba.com/press.html?id=9

1. The Hopkins Report

In early 2003, much of the source code for Diebold's AccuVote TS system was accidentally released on the company's own open FTP site. Professor Avi Rubin, an internationally respected security researcher at Johns Hopkins University, and his colleagues, used this data to conduct the first independent study of the security of a DRE voting system with access to the source code.

The study was not peer reviewed before its first publication, and the authors have softened a few of its conclusions since then. However, its overall conclusions still amount to an extremely harsh judgment of the security features in the Diebold AccuVote TS system. Those conclusions were largely validated by the three subsequent reports that we will summarize below.

The authors of the report state in no uncertain terms their concern:

> Our analysis shows that this voting system is far below even the most minimal security standards applicable in other contexts. We identify several problems including unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, and poor software development processes.

They go on to add:

> Furthermore, we show that even the most serious of our outsider attacks could have been discovered and executed without access to the source code. In the face of such attacks, the usual worries about insider threats are not the only concerns; outsiders can do the damage. That said, we demonstrate that the insider threat is also quite considerable, showing that not only can an insider, such as a pollworker, modify the votes, but that insiders can also violate voter privacy and match votes with the voters who cast them. We conclude that this voting system is unsuitable for use in a general election.

The authors conclude with their most significant recommendation:

> We suggest that the best solutions are voting systems having a 'voter-verifiable audit trail,' where a computerized voting system might print a paper ballot that can be read and verified by the voter.

Although this report was very controversial at the time it was issued, the authors are very well qualified and respected. Their results and recommendations merit careful consideration.

2. The SAIC Report

At the time of the publication of the Hopkins Report, the State of Maryland was in negotiations with Diebold for a statewide procurement of its Accuvote TS machines, the very ones studied by Rubin and his colleagues. Because of the controversy engendered by the Hopkins Report and its sharp criticism of the Diebold system, the state requested the nationally prominent technology consulting firm SAIC to make a second examination of the system and make recommendations.

SAIC issued its report in 2003. About two-thirds of that report was redacted before it was made public. This discussion is based on that redacted version.

The SAIC report took issue with some of the findings in the Hopkins Report, stating that:

> In the course of this Risk Assessment, we reviewed the statements that were made by Aviel D. Rubin, professor at Johns Hopkins University, in his report dated July 23, 2003. In general, SAIC made many of the same observations, when considering only the source code. While many of the statements made by Mr. Rubin were technically correct, it is clear that Mr. Rubin did not have a

> complete understanding of the State of Maryland's implementation of the AccuVote-TS voting system, and the election process controls or environment. It must be noted that Mr. Rubin states this fact several times in his report and he further identifies the assumptions that he used to reach his conclusions. The State of Maryland procedural controls and general voting environment reduce or eliminate many of the vulnerabilities identified in the Rubin report.

Nonetheless, the SAIC report goes on to enumerate 17 serious vulnerabilities in the Diebold AccuVote-TS system that were identified as having a "high" risk rating. It states in summary:

> This Risk Assessment has identified several high-risk vulnerabilities in the implementation of the managerial, operational, and technical controls for AccuVote-TS voting system. If these vulnerabilities are exploited, significant impact could occur on the accuracy, integrity, and availability of election results… This Risk Assessment also identified numerous vulnerabilities with a risk rating of medium and low that may have an impact upon AccuVote-TS voting if exploited.
>
> * * *
>
> The system, as implemented in policy, procedure, and technology, is at high risk of compromise.

The SAIC report took issue with a limited number of the Hopkins Report findings and did not assert that the Diebold systems were unfixable. Accordingly, Diebold claimed publicly that report was vindication of the security of the AccuVote TS. Taken as a whole, however, the report is critical of the security of the AccuVote TS system.

3. The Compuware Report

Shortly after the SAIC report was released, the State of Ohio commissioned another consulting firm, Compuware (and two subcontractors, InfoSENTRY and RJV), to examine the security of four vendors' systems in order to help make a voting system procurement decision.

The Compuware report is the most detailed of the four reports, and it is the only one to evaluate four different voting systems. The report contains a detailed description of each system examined; indeed this report is probably the best single source for this cross-vendor information. The report is divided into four major parts, one for each vendor. Each part is based on an established risk management evaluation process: characterization of the threat, analysis of the threat, vulnerability identification to the

determination of risks (high, medium, or low), strategies for risk mitigation, and documentation of results.

While the Compuware report provides a highly detailed analysis of each individual system, the report fails to compare the relative security problems it found with the four systems it analyzed. Rather, for each system analyzed, the report concludes with a paragraph that is essentially identical to the following:

> During the course of our study, Compuware identified several significant security issues, which left unmitigated would provide an opportunity for an attacker to disrupt the election process or throw the election results into question. These are documented throughout this assessment report. Following careful consideration of each of these security issues, we developed mitigation recommendations for the Secretary of State to implement which we believe will limit the likelihood of a successful attack or inadvertent disruption to the election process. Provided that mitigating strategies are executed for each risk identified before the systems are used in an election, Compuware concluded that the Secretary of State can securely deploy these voting machines."

It would have been much more useful if the Compuware report had done a detailed compare-and-contrast analysis of the four, indicating which ones are superior or inferior based on specific criteria.

Finally, the Compuware analysis of the four voting systems is not as critically rigorous as that employed by as Hopkins and RABA authors. The Compuware report does not characterize any vulnerability as characterized as "high risk," as being due to poor design, or based on the failure of the system designer to understand security principles adequately. Finally, the report appears to give no serious consideration to recommending that one or more of the systems might not be ready for deployment, rather than proposing ways to minimize the risks it did identify.

4. The RABA Report

Even though the Diebold system had been evaluated by external reviewers in the three previous reports, the Maryland government late last year commissioned yet another report on the security of the system, this time from a small security firm called RABA Technologies, whose principal have strong connections to the National Security Agency. In part, the RABA team's charge was explicitly to evaluate the Hopkins and SAIC reports, as well as the Diebold AccuVote TS system itself.

The RABA investigation was technically the most thorough of the four. In particular, it involved a "red team" exercise in which the conditions of an actual election are simulated, and a team of technical experts attempts various attack scenarios in order to compromise the system.

The conclusion of the RABA report, like those of the other three reports, was that the Diebold Accuvote TS system has a number of security vulnerabilities. In the Executive Summary the authors wrote:

> "The key findings of this effort are two-fold. The State of Maryland election system … contains considerable security risks that can cause moderate to severe disruption in an election. However, each of these vulnerabilities has a mitigating recommendation that can be implemented in time for the March 2004 primary. With all these near-term recommendations in place, we feel, for this primary, that the system will accurately render the election and is worthy of voter trust. However, between the March and November elections we strongly feel that additional actions must be taken to mitigate increasing risks incumbent on a system that will receive broad scrutiny. Ultimately, we feel there will be a need for paper receipts, at least in a limited fashion."

The authors of the RABA report were critical of Diebold's security architecture. They concluded that Diebold's software could not be brought to the level of "best practice security" just by upgrading it, or fixing a specific list of identified problems. Instead, they call for a complete re-write of the source code:

> "It is our opinion that the current DIEBOLD software reflects a layered approach to security: as objections are raised additional layers are added. True security can only come via established security models, trust models, and software engineering processes that follow these models; we feel that a pervasive code rewrite would be necessary to instantiate the level of best practice security necessary to eliminate the risks we have outlined in the previous sections. Our analysis lacked the time and resources to determine if DIEBOLD has the expertise to accomplish this task."

Taken together, the four reports paint a disturbing picture of the security of the electronic voting systems considered in their studies.

B. Security Issues Related to the March 2, 2004 Election.

The March 2, 2004 election provided the first large-scale implementation of this new technology, with 14 counties using these systems at precinct polling places (See

Appendix III – List of Counties Using Touch screen Voting Equipment in the March 2, 2004 Election). As the four reports discussed above make clear, as the use of touch screen voting systems has increased, so too have concerns regarding their security.

In the face of these concerns, and in light of the just released RABA report, on February 5, 2004, the Secretary of State advised counties using touch screen voting equipment of existing procedures and additional security measures necessary to assure the security of the March Primary. (See **Appendix IV** – Security Measures for Touch screen (DRE) Voting Systems for the March Election.) On February 24, 2004, the Secretary provided additional information and clarification to counties concerning security measures (See **Appendix V** – Election Day Information and Updates), including the assurance that counties would not have to bear the costs of the additional security measures. These measures were specifically designed to provide additional security and voter confidence in the voting process until implementation of the Secretary of State's requirement that all DRE voting systems include a voter-verified paper trail.

The measures included requirements that:

- each county and each voting-system vendor prepare an Election Security Plan;
- counties have an Election Observer Panel Plan addressing the public observation of the election process;
- counties comply with new rules relating to the pre-election "Logic and Accuracy" testing of voting equipment;
- counties submit to the Secretary of State the membership of its Logic and Accuracy Board;
- a copy of the software each county uses to tally ballots be submitted to the Secretary of State;
- counties utilize tamper-proof seals on all equipment ports where memory cards are inserted;
- counties implement "smart card" security procedures;
- counties have their Election Day troubleshooters look for evidence of tampering with voting equipment as they inspect polling places;
- a copy of the results from each polling place be publicly posted at that polling place in order to assure the public that the votes recorded at the polling place were not altered en route to the elections office;
- prohibited the use of wireless technology;
- each county use at least two persons to transport vote results to county election offices;

- the premises where votes are tabulated and the tabulated vote results be secured; and,
- counties back-up electronic files of vote totals.

Four counties were of particular concern – San Diego, San Joaquin, Kern, and Solano – because they used a touch screen system that was only conditionally certified for use in California. That system, the Diebold AccuVote-TSx system, has yet to receive full federal qualification. Recognizing that Diebold had already installed the system in the four counties and had modified the system since it received conditional certification, federal and state testers recommended the system be used only for the March Primary. (Certification issues relating to the Diebold TSx system will be addressed at greater length in another report that will be issue in connection with the VSPP meeting on April 21 and 22, 2004.)

As a result, on February 11, 2004, the Secretary of State issued additional security directives to these four counties (See **Appendix VI** – Use of AccuVote TSx Voting Systems in March.)

Specifically, as an additional means of strengthening the security of the touch screen systems, the Secretary of State directed that a paper record of each vote be captured to assist in resolving post-election issues regarding AccuVote TSx machines.

With respect to all the additional security measures mandated by this office, a number of counties initially resisted. In the end, however, the vast majority of the counties complied with most of the measures. Of particular concern, however, were:

- Kern County, which did not print a paper record of the cast ballot images;
- Eight of the 15 counties using touch screen machines did not submit Election Security Plans to this agency;
- Eight of the 15 counties using touch screens did not submit County Election Observer Plans to the Secretary of State.
- Five counties, Alameda, Kern, Plumas, San Diego and Shasta, failed to post results at the polls after the election; and
- Alameda and San Bernardino County refused to provide a record of the vote on CD-ROM or DVD to the Secretary of State.

Despite most counties' implementation of the unprecedented security directives, questions about security persist. Security of voting systems is comprised of two areas: technical security and physical security. Technical security is the ability of the equipment to prevent tampering with its software and firmware. Physical security addresses how resistant the machine is to external factors such as tampering to the

hardware, environmental degradation (such as from jostling, water damage, etc.), and even how secure the room or facility is that stores the machines.

While most counties implemented these procedures as directed by the Secretary of State, which addressed both technical and physical security, the widespread view was that technical security was the larger risk. However, after observing the administration of the March Primary, it has become clear that physical security is also an issue that must be addressed.

In the past, the physical security of voting machines consisted of storing the ballots in secure locations to ensure that they are not subject to tampering or theft. But individual machines, particularly punch card machines, were not at great risk of tampering because the machines were simply a device used to hold the ballot and enable a voter to correctly punch holes in the ballot to mark their votes. With touch screen machines, the issue of physical security of the devices is more significant, and larger questions arise. Many voters have expressed concerns about the physical security of the machines, once out of the hands of the elections officials.

For instance, a Secretary of State observer noted that, like other counties, San Diego delivered its touch screen machines to polling places or pollworkers several days before the election, providing all pollworkers the passwords to the machines. This was an issue that this agency's directives should have, but did not, address.

One observer questioned the possible breach of security inherent in this practice. This was also questioned by a San Diego pollworker who testified before the Board of Supervisors at a hearing after the election. As noted in a caption of a photo accompanying a March 17, 2004 San Diego *Union-Tribune* article by Helen Gao, "Encinitas polling (sic) worker Jennifer Hamilton showed county supervisors seals and zip ties used to secure voting materials in the March Primary. She said the items are inadequate for the task." Finally, during her testimony, she reported that the "tamper-proof" tape had curled on its own and was not actually tamper-proof and capable of clearly revealing that the machine had been tampered with. Again, the Secretary of State's Office should have provided more specific guidance on this issue.

These aspects of physical security must be examined in greater detail by the Secretary of State's Office in order to provide guidance or statewide standards for assuring the physical security of voting machinery through the entire chain of custody from the county offices to the polling places and back.

With regard to technical security of the touch screen systems in use on March 2, 2004, it is clear that none of the systems is completely equipped to deal with all potential

security breaches. Indeed, some are less prepared than others. However, the fact that security questions can be and have been raised at all for systems that have undergone federal qualification testing and that received state certification reveals a singular fact: The testing regimen is not as complete as it needs to be. Finally, without a paper audit trail that allows contemporaneous voter verification of his her choices, many forms of tampering could not be discovered. Without such a system, if such tampering did occur, it may prove impossible to reconstruct voter intent.

C. Parallel Monitoring.

On March 2, 2004, Secretary of State staff conducted a parallel monitoring program as an additional means of examining the accuracy of touch screen systems used in the election. As requested, eight counties participated in the parallel monitoring project. Parallel monitoring consisted of testing electronic voting machines from all vendors certified in the State of California. This was the first time such testing was done in any election.

Parallel monitoring is an important security precaution, particularly in the absence of an accessible voter-verified paper audit trail (AVVPAT). The parallel monitoring process is specifically designed to detect the potential presence of *malicious code* in the software of a voting machine that would otherwise not be detected by other testing processes.[2] An accessible voter verified paper audit trail eliminates concern about malicious code, which is one of the reasons that the Secretary of State has required it in California by 2005 for new systems, and by 2006 for all systems.

Under the parallel monitoring procedures, two touch screen machines of each model used by a California county on Election Day were randomly selected and removed shortly before the election to be tested. Because the Diebold TSx system had only conditional certification, a total of eight TSx machines (two from each county using the system) were selected for the parallel monitoring process.

Voters did not use these machines at the March Primary. Instead, they were test-voted on Election Day in a simulated election conducted at the same time and in the same manner as the actual election. Parallel monitoring minimized the risk that malicious software would detect that the machines were not being used by actual voters, and thus not execute its malicious code. All test-votes cast were videotaped to compare the

[2] Malicious code is software deliberately and secretly inserted into a computer to make it malfunction, either by failing to properly do the job it is supposed to do, or by secretly doing extra things it is not supposed to do. Sophisticated malicious code is designed to be *hidden*, so that people reading the code cannot easily find it; and it might also be designed to *resist detection by testing.* It is important to distinguish malicious code from ordinary *bugs*. Bugs are honest mistakes made by programmers, and they are not deliberately hidden, nor specifically designed to resist detection.

results reported by the machine against the votes actually entered on the machine by Secretary of State testers. Any unresolved discrepancy found during this procedure would indicate the presence of potential malicious code in the voting machines.

The parallel monitoring tests confirmed that the test-votes cast were accurately recorded on each of the tested touch screen machines. The Parallel Monitoring Program indicates that the 16 touch screens that were tested on March 2, 2004 accurately recorded the votes as cast.

The parallel monitoring program, however, was limited in its scope. Parallel monitoring is only able to assess the ability of the software tested to generate accurate results from the votes entered. Parallel monitoring was not designed to detect whether all touch screens used at the March Primary recorded votes accurately. Nor does it exclude the possibility that other sequences of votes or behaviors might trigger a different result.

Moreover, parallel monitoring does not address whether (a) touch screen machines were running firmware with uncertified modifications or patches, (b) security holes exist in the firmware that could be exploited, (c) machines in use on Election Day were tampered with and/or used in a manner that exploits such security holes, or (d) systems tabulating the votes were tampered with, apart from the accuracy of the DRE machines.

Although the results of parallel monitoring were encouraging, the program cannot provide guidance for future elections. Again, absent an accessible voter-verified paper trail, parallel monitoring must be repeated for every election with every type of touch screen system being used in the state.

A more complete parallel monitoring report can be found on the Secretary of State website at http://www.ss.ca.gov/elections/touchscreen.htm.

V. TRAINING

The March Primary demonstrated that when touch screen machines experience a problem, pollworkers often do not have the technological expertise to resolve the problem unless they have received specific training on that issue. This training issue is compounded by the fact that, in many cases, manufacturers have failed to provide adequate documentation and training about their systems to elections staff, and that many of the error messages generated by the machines provide no information about how to fix the problem. And when vendors introduce new devices, or modify software or firmware, on the eve of the election after pollworker training is completed – and often and without adequate testing – the result is predictably troubling.

In examining the issue of training in connection with the use of touch screen systems in the March Primary, we examined not only whether pollworkers were adequately trained to operate the systems when those systems performed as expected, but also whether pollworkers were able to quickly and easily correct problems that did occur. Although most reports suggest that pollworkers generally were able to operate touch screen systems when they performed as expected, many problems arose that either pollworkers could not easily resolve.

A. San Diego County

Although the primary problem with the Diebold PCM-500 failure was a result of the equipment itself, it also revealed a critical training issue related to the use of touch screen voting, especially new equipment installed close to an election. Most pollworkers were not trained to address this problem by either Diebold or the county. Moreover, the equipment itself was not sufficiently user-friendly to allow pollworkers who lacked computer experience to assess and adequately correct the problem without adequate training. A dialogue box or icon for the program that provided direction on how to start the encoding software on the machine would have been useful. Instead, the problem baffled a significant number of pollworkers and seriously disrupted the county's election.

B. Orange County

The issue of pollworker training for DRE systems was also an issue in Orange County, where pollworkers provided many voters with incorrect ballots. Where multiple voting precincts with different ballot types were located at the same polling place, pollworkers had to carefully use the DRE voting equipment in order to provide voters with the appropriate electronic ballot. If the pollworker made the wrong selection, the voter could receive the incorrect ballot.

C. Tehama County

Some pollworkers experienced difficulty in powering down the touch screen machines. Pollworkers had to be walked through the process and eventually all machines were properly powered down.

D. Kern County

Some pollworkers did not keep the card encoders plugged in on election day, which caused their PCM devices to revert to a Windows screen instead of the

"issue ballots" screen. In addition, the county reported four instances where inspectors improperly left memory cards in touch screen units.

E. Napa County

Several touch screen units were not shut down properly. In some cases, the pollworkers failed to remove the memory cards from the touch screen units.

Recruiting, training, and retaining pollworkers is a challenge for every local election official. This is particularly true in counties such as Yuba and Sutter, whose registrars were conducting their first presidential primary election. Attracting individuals to work for long hours with low pay is difficult. Many counties have sought to use local businesses, governments and community organizations to help them recruit pollworkers. But a majority of California's registered voters did not even cast a ballot on March 2, 2004, so it is clear that finding people to serve as pollworkers is even more daunting.

In seeking to ensure an adequate supply of pollworkers, counties used a number of approaches. For example, Alameda was one of the counties that utilized a significant number of student pollworkers as now authorized by the law. Many counties used county employees as pollworkers. Solano County relied on the extra assistance of county employees during the busiest times at its polling places.

In January, legislation sponsored by the Secretary of State was enacted to improve and standardize pollworker training statewide. Pursuant to this legislation, the Secretary must create a task force that includes local elections officials to craft statewide standards.

Over the longer term, implementation of these statewide standards will improve pollworker training in California, and presumably touch screen systems will become more stable and user friendly. But that provides little comfort about the adequacy of training for pollworkers in touch screen counties for the November 2004 election. Between now and the November election, new components will undoubtedly be added to touch screen systems, and their software and firmware will be modified. As revealed by the PCM problem, problems created by those changes may not be discovered until election day. So, even though pollworkers can be trained to handle the problems that plagued the March Primary, new problems will arise in the November 2004 election, and poll workers may be no better able to fix those problems than they were the PCM problem.

CONCLUSION

Touch screen systems are a promising technology and offer a number of potential benefits to California voters. However, the events surrounding the March 2, 2004 election discussed in this report also raise substantial questions about present touch screen systems' reliability, accuracy and security. DRE technology also presents new challenges for pollworkers, and requires additional pollworker training and recruitment efforts.

The number of last-minute vendor requests to approve modifications to these new systems suggests that the technology is still evolving and not entirely stable. These numerous requests for modifications also reveal that the state and federal testing and approval processes must be strengthened.

The immediate issue is whether the problems experienced with DRE systems, together with the known security issues, can be resolved adequately in time for the November 2004 election. An accessible, voter verified paper trail would address the most significant security concerns, and give voters greater confidence that their votes will be recorded and counted accurately. It is unclear at this time, however, whether AVVPAT will be available in time for the November 2004 election.

Staff makes no recommendation regarding whether DREs should be used in November if a paper trail is not available; that issue will be the subject of a Voter Systems and Procedures Panel hearing on April 21 and April 22, 2004. Plainly, however, moving the implementation date for mandatory AVVPATs from June 2005 back to November 2004 should be considered.

The DRE issues identified in this report provide a useful roadmap for necessary changes to DRE technology, the certification and testing process, training, and election laws. In particular, staff recommends the following:

Certification and Testing

- ✓ The Secretary of State's Office should not allow the use of equipment or software without full federal testing and qualification, source code review, and review by the Secretary of State's Voter Systems and Procedures Panel (VSP) whenever a significant change is made.

- ✓ Voting system vendors should not be permitted to submit applications for approval at the last minute. Rushing the testing process increases the chance full testing will not be complete, and encourages additional last-minute applications.

The Secretary of State should establish firm application deadlines for certification of voting systems and software for the November 2004 election.

- ✓ All systems certified under the federal 1990 Voting System Standards should be retested to meet the standards of the 2002 standards. In addition, all systems that were in use before federal qualification testing began in the mid-1990s should be retested as well. For statewide elections in 2006, all voting systems should be compliant with the 2002 federal standards and certified to California's state standards.

Reliability

- ✓ Each year, after new election laws are enacted, vendors should provide a demonstration and report confirming their systems can adequately implement the new laws, assessing whether modifications need to be developed, and establishing a timeline for submitting such modifications for review. Where possible, vendors should develop alternative procedures to accommodate the change in law without modifications in the event that the modifications proposed do not meet federal or state requirements.

- ✓ All polling places using DRE systems should be supplied with back-up paper ballots. This would permit voters to cast their ballots even if electronic equipment fails, and permit voters who are uncomfortable with DREs for any reason an alternative means of voting.

- ✓ In the absence of a voter verified paper audit trail, all counties using DRE systems should be required, as part of the official canvass of the vote, to print out on paper a complete copy of the images of the voted ballots cast on each DRE machine used in the election. The paper record should be used for the one percent manual recount to audit the machine-tabulated total, and in any request for a full manual recount.

- ✓ Counties using DREs should be required, as part of the semi-official canvass, to produce at least four original CD-ROMs or DVD-ROMs containing images of the voted ballots cast on each DRE machine used in the election. Two copies should be filed with the Secretary of State and two should be kept on file with the county elections official.

Security

- ✓ This office should require that all DRE voting system vendors seeking certification implement the security recommendations made in the SAIC, RABA and Ohio reports, or take other similar measures, to address the security deficiencies highlighted in those reports. All vendors should be required to report to the Secretary of State the manner in which they have addressed the recommendations of the reports.

- ✓ Attention should be paid to the physical security of DRE voting systems and the chain of custody that each DRE follows from the county elections office to poll workers to polling places and back. The Secretary of State should utilize a third party to conduct an evaluation of physical security of DREs and to develop guidelines for counties to maximize physical security of their systems.

- ✓ Vendors should be required to develop a system to permit the Secretary of State to authenticate the code in each DRE machine by affixing a digital signature to the code once it is certified. The version with the digital signature should be compared to the version that was federally qualified. The digitally signed version should be the only version installed on systems in California and the Secretary should establish spot checks to assure compliance.

- ✓ The Secretary should seek legislation making it a felony to gain unauthorized access to a voting machine for the purpose of tampering with the system. This legislation should also make it a felony to insert uncertified hardware, software, or firmware into any voting system.

- ✓ In addition, the Secretary of State should seek legislation authorizing the Secretary, Attorney General, and local elections officials to bring a civil action against anyone who tampers with a voting system or individual voting machine. The legislation should also make it a felony for a vendor to fail to notify the Secretary of State prior to any change in hardware, software, or firmware to a certified voting system.

- ✓ Finally, the Secretary of State should pursue legislation to authorize fines and sanctions against any voting system vendor that violates the state's voting system certification laws and procedures.

Training

- ✓ Adopt statewide poll worker training standards that require minimum time for each trainee on the systems they will operate on Election Day.

- ✓ To ensure accessibility of a system, require an evaluation by disabled voters before certification is granted. This would provide real-world feedback on the ease of use of the system.

- ✓ Require directions at the end of each DRE screen page to continue to another page or to continue scrolling.

Finally, the Secretary of State should call upon the Legislature and Governor to allocate more funding to implement these recommendations, to approve training and hiring of more technical staff and to ensure the security of our voting systems is the best possible.