2003-2004 SANTA CLARA COUNTY CIVIL GRAND JURY

INQUIRY INTO COUNTY ELECTRONIC VOTING SYSTEM

Summary

The 2003-2004 Santa Clara County Civil Grand Jury (Grand Jury) investigated the recent adoption by Santa Clara County (County) of touch screen electronic voting machines. As a result of its inquiries, the Grand Jury found several problems with the physical security of the electronic voting machines and with the handling of the equipment but, in general, felt that the Santa Clara County Registrar of Voters (Registrar) was providing voters with a reliable and secure method of voting. However, due to press reports and statements by concerned citizens and electronic voting critics, there has developed among some of the public an apprehension that this system may be unreliable. In fact, this perception is so pervasive that the only way to restore public confidence in electronic voting by touch screen computers may be through the implementation of a paper trail for each vote cast. Such a paper trail has now been ordered by the Secretary of State and will be in place by mid-2006.

The Grand Jury found that electronic voting would improve the reliability of election results compared to previous punch card systems with six caveats:

1. The Grand Jury found problems with the physical security of the electronic voting machines and the handling of the equipment. The Grand Jury recommends improvement in these areas and continued vigilant monitoring of voting security.

2. Due to the non-transparent nature of the technology, a portion of the public has the perception that electronic voting is unreliable, because of malfunctions and perceived undetectable computer fraud. This apprehension can be eased, in part, by the adoption of an individual paper record of each vote, verified by the voter, and available for a hand recount if necessary. The paper trail itself is similar to liability insurance—you hope you never have to use it, but it is there when needed. This enhancement has been part of the County's plans, is included in the electronic voting machine vendor's contract, and is now required by the State of California to be in place by mid-2006.

3. The creation of a paper trail raises new problems for disabled voters. Electronic voting machines with audio capabilities were designed to put disabled persons on an equal footing with the non-disabled. The creation of a paper trail introduces a new problem in that sighted persons, being able to verify their ballots, will have an advantage over the sightless. This inequity should be resolved before electronic voting machines with paper trails are approved for general use.

4. The Registrar should provide an alternative paper ballot to those persons who cannot or refuse to use electronic voting machines.

5. The Grand Jury finds that continuous public oversight of the process needs to continue to ensure valid elections. The checks and balances around elections that have grown up over the years need to be further refined to take into consideration the electronic nature of the new voting machines. An ad hoc group of experienced computer engineers can be of invaluable help in monitoring and searching for ways to prevent fraud in all aspects of electronic voting.

6. Any ballot system, whether it is based on paper, old-style mechanical voting machines, optical readers, punch cards, absentee ballots, or electronic voting machines, is subject to manipulation by those both inside and outside the process. The integrity of the voting system depends primarily on the honesty and competency of the people involved, along with proper safeguards, ***especially*** to prevent unauthorized access to any part of the system. Only vigilant monitoring of all phases of an election, from voter registration and verification through reporting of totals, can suppress vote fraud and mistakes.

As a side issue, the Grand Jury found that the increasing use of absentee ballots could be a negative factor for the general security of the entire voting operation. Absentee ballots are outside the control of the Registrar during many steps of the process, and thus are subject to a large number of possible problems, including the sale of votes.

Background

The widespread problems connected with the 2000 election in Florida, including the use of punch card machines, brought the issue of antiquated voting methods to the attention of the public. The federal government encouraged reform with its Help Americans Vote Act (HAVA) in 2002, authorizing $3.9 billion to aid state and local governments in modernizing their election systems.

Until November 2003, the County used a punch-card system similar to that at issue in Florida. Working with a citizens advisory committee and computer experts, the Registrar approved an $18.9 million contract with Sequoia Voting Systems for 5,500 electronic voting machines. Competing with Sequoia were Election Systems and Software, Inc. and Diebold, Inc., both of which have been the recent targets of considerable criticism.

The Grand Jury was particularly impressed by the extent of citizen participation in the process of selecting and implementing the use of electronic voting machines. From the start, citizens have helped the Registrar select a system, develop guidelines for its use, and monitor the results.

However, on April 30, 2004, the Secretary of State, in an order banning the use of Diebold touch screen voting systems in four counties in California, also notified the ten remaining counties in California using touch screen systems (including Santa Clara) that they would have to either install a voter-verified paper trail before the November election or meet 23 security measures before he would recertify those systems. The Registrar reported to the Grand Jury that he has already, or will be able to meet all of the security measures that are the responsibility of the county and fully expects to be using electronic voting machines in the forthcoming November

election. However, if Sequoia chooses not to supply its source code to the Secretary of State or pay for the paper ballots and the Secretary of State does not withdraw these requirements, then the electronic voting machines cannot be used in the November election.

Discussion

In August, 2003, the Grand Jury began an inquiry into how well the County is adjusting to a new voting system and how reliable and secure such a system is.

The inquiry began two months before the November election, which marked the debut of electronic voting machines in the County, and included the March primary election. Members of the Grand Jury interviewed the Registrar several times, visited the machine holding area and watched the machines being programmed for the upcoming elections, discussed security problems with members of the Registrar's staff, sought comments from concerned citizens and voting machine critics both pro and con electronic voting, observed the security surrounding the delivery of the machines, attended a debriefing of polling day inspectors, and questioned the Registrar and his immediate staff on the success and failure of the electronic voting machines. Numerous documents, letters and opinion pieces were reviewed.

This report does not attempt to report on all of the technical problems associated with electronic voting machines. Media from around the country have given considerable play to stories, some anecdotal, of problems with electronic voting such as vulnerability to outside tampering, server errors, and computer glitches which, in one reported case, changed votes from Democratic to Socialist. There have been no complaints with the way the County Sequoia system was implemented. Many of the technical problems have been explored in depth in two major studies, one by the Congressional Research Service of the Library of Congress and another by the Ad Hoc Touch Screen Task Force created by the California Secretary of State. The Grand Jury does not wish to duplicate these works, nor does the Grand Jury have the expertise to discuss in much depth the problems and solutions associated with computer technology.

The most serious problem for any system was the possibility of intentionally recording results that did not reflect the voters' intentions. This led to the formation of other impromptu groups of computer gurus who demanded a paper trail that could be used to manually recount the vote of a specific machine(s) if the count was in doubt and, more importantly, would allow the voter to see a printed list of their votes before completing the voting process.

When the County's 5,500 electronic voting machines were originally ordered, they were not equipped with a paper trail mechanism. The electronic voting requirements listed by the federal and state governments did not require a paper trail, but the Registrar foresaw that such a system might be required in the future and his initial contract with the machine suppliers allowed for a paper printer to be added in the future at no additional cost to the County.

Debate has produced two distinct groups among some members of the voting public: those in favor of a paper trail and those who felt it was not necessary. The debate revealed a deep divide

between those who trusted the new system and those who mistrusted it. It was a debate largely played out in the media and lacked any significant input from the manufacturers of the machines.

The November election, which only involved a third of the precincts, was a critical test for those promoting the touch screen approach with no paper trail. Unlike several other counties, which had to deal with a variety of problems, the Santa Clara County election ran like clockwork and few complaints were registered.

At the state level, the concerns about the security of electronic voting machines overcame the objections concerning the reliability and maintenance costs of printers. On November 21, 2003, the Secretary of State ruled that beginning July 1, 2005, all new machines must have a paper audit trail and every system in use after July 1, 2006, must incorporate a paper trail. These paper trails must be kept within the machine since federal law prohibits voters from taking from the polling place an official record of how they voted.

The Registrar and the Secretary of State must, by law, approve any changes to voting machines, including the addition of a printer. The Grand Jury recognizes that computer printers are not always reliable (paper can break or jam, ink can run out, etc.) and feels the exact form the paper trail takes is better left to the machine designers. However, it envisions a paper printout, similar to the receipt used by supermarkets, showing a summary of votes cast that replicates what is shown on the touch screen summary. This must be kept inside the machine, perhaps under a glass, so it is easily read by the voter, and any printout must randomize the votes so that no vote can be connected with an individual voter.

The integrity of the voting process is fundamental to the operation of our democracy and every effort must be made to avoid even the appearance of corruption in our voting system. A major component of a valid electoral process is voting technology that honestly and accurately counts every ballot. Since voting technologies have always been susceptible to error, bias, and corruption, a democratic society must strive to maximize the likelihood of recording what each voter intends. And, because our form of government requires that the public have confidence in the results of elections, voting technologies must ensure that elections cannot be rigged in a way that would thwart the true will of the electorate.

The introduction of touch screen electronic voting machines produced new problems. Other states and counties have experienced problems in setting up the machines and in training of poll workers and others responsible for overseeing the use of the machines. There were instances in which manufacturers have not lived up to their representations concerning the machines, including in other counties of California. There were claims that some state and County officials are too close with the manufacturers of the machines and that there is a revolving door between the two. There have been reports of machine malfunctions and vote totals not being correctly recorded.

Of course, not all reports of voting machine problems are accurate. One case that the Grand Jury investigated was a remark in a public meeting by a poll worker that three of five machines failed at one site during the March 2004 Election, and worse, that the number of voters who had signed in was 15 less than the number of votes recorded by the machines. It turned out that one machine

had a screw lose and was removed from service. Two machines needed the touch screen sensitivity adjusted to work with long fingernails. Neither problem caused extra votes to be recorded. Regarding the 15 missing names, the poll workers had overlooked signatures in a supplemental roster.

Current commercial electronic voting machine software code is proprietary and not subject to public scrutiny. A local non-profit group of software engineers and computer scientists, the Open Voting Consortium, formed to assess the range of threats to electronic voting security and to promote publicly accessible voting-machine software. Based on the prototype demonstrations they have now, it would be at least several years before any commercial open-source systems could be available and certified.

Another problem noted by the Grand Jury was security of the voting machines when not in use. In the Registrar's office on Berger Drive, the machines are stored behind a floor-to-ceiling chain link fence. Access is controlled by the color of an individual's badge—only those wearing a badge of a certain color are allowed inside the fenced area without an escort. However, what is lacking is any sort of written record of who enters the area and the date/time. The coded badge system would probably work if there were a guard posted at the gate; there is not, so the only control is if someone saw somebody with the wrong badge color within the area. The loading room, where the cartridges are made for the individual machines for each election, has an electronic lock, but no record exists showing who entered the room and when. These are the most sensitive areas connected with the voting equipment; they both should have electronic locks and a log of everyone who enters and leaves the areas.

Recently, security cameras were installed in these areas with tapes from these cameras monitored and kept by a department other than the Registrar. The tapes can be screened to see if any unauthorized personnel were present.

Several days before the election, a private trucking company delivers the machines, loaded with the cartridges for the specific election, to the various polling places around the County. Depending on the site, the machines are either transferred immediately into the area to be used for the polling place or left somewhere on the site. Members of the Grand Jury found some of these machines sitting in a teachers' lounge at a private school, next to a window of a semi-abandoned gym, and just inside a fire station garage area, open to the public when the fire fighters were on a call.

Even though it is difficult to tamper with these machines, anyone intent on damaging the machines would find this situation inviting, although it is extremely difficult to alter a machine. For example, after the machine is at the polling place, if the cartridge is removed and replaced, altered or not, the machine automatically locks and cannot be used without being reprogrammed at the warehouse. The machine also is taken out of service by the poll workers if the counter is not at zero when it is opened and inspected on election day. To prevent problems that could delay opening of the polls, the voting machines must be secure at all times.

When the voting machines leave the Registrar's warehouse, the controls are locked with a numbered plastic seal. The Grand Jury found, however, that in the November election, no record

was kept of the seal numbers, thus leaving open the possibility that the seals could be removed and later replaced without election officials knowing what had happened. This problem was corrected before the March election by having the seal numbers given to poll workers who checked the numbers before activating the machines.

The Grand Jury did not explore in depth the possibility of electronic tampering with voting machines from outside sources. As long as the machines stand alone and have no external connection such as to the Internet or telephone system, they are, by today's technology, basically impervious to such tampering, except by insiders. The Grand Jury felt this requirement was basic to the security of the voting machines and system; the Registrar assured the Grand Jury there are ***no*** plans to connect the voting machines to any outside source. All transfer of data will be through the physical transfer of data cartridges.

There is, of course, the possibility that someone anxious to alter the software inside the voting machines could infiltrate the Registrar's staff. While the Grand Jury believes the chance of this taking place is remote, it is possible, and this possibility requires that the Registrar be constantly alert and conduct regular audits of the machines' software.

For some years to come there will be voters who are uncomfortable with electronic voting, for one reason or another. The Registrar should make an alternative system available by allowing voters to use paper ballots at polling places.

While the Grand Jury understands the desire of the Registrar to encourage absentee voting (early absentee voting allows the Registrar to process and count absentee ballots before the rush of election day tallying), it is greatly concerned over the lack of security for absentee ballots. The ballots are completely unprotected from the time they enter the postal system to when they are delivered to the voter, and later when mailed by the voter to the Registrar. The voter has no assurance that the ballot was received by the Registrar unless some type of verification such as a posting on the Registrar's website or a dedicated phone line is available to the voter. Also, one of the legal requirements that make a paper trail system more complicated is that, to inhibit the selling of votes, it must not let the voter leave with a record of the votes cast. Yet, with absentee ballots, the intent of that law cannot be enforced. The possibility of tampering with the ballots is great enough to cause the Grand Jury concern, particularly now that the number of absentee voters in the County has increased to almost one-third of all votes cast.

Finding I

Every voting machine is subject to manipulation by those inside or outside the process.

Recommendation I

The Registrar must vigilantly monitor all phases of the election process with continuous oversight to suppress fraud and mistakes.

Finding II

Many computer novices, handicapped persons, and non-English speakers are uncomfortable with touch screen voting.

Recommendation II

The Registrar should continue public education about electronic voting, with particular attention to non-English speakers and handicapped voters.

Finding III

At the Registrar's Office, in both the loading room and the general storage area for the machines, although a video record is kept, there is no electronic record of who enters, how long they are there or when they leave.

Recommendation III

The Registrar should increase security on machines in both the loading room and the general storage area. The Registrar should install electronic locks on the storage area and provide an electronic signature record of who enters and leaves each area.

Finding IV

Loaded voting machines were delivered to polling places by a private trucking company and, in some cases, appear to have been left in unsecured areas.

Recommendation IV

The Registrar should not allow the machines to be left unsecured. All deliveries should be immediately placed in a secure area.

Finding V

The lack of a paper trail has caused many people to distrust electronic voting equipment.

Recommendation V

The Registrar should expedite the planned installation of a paper trail on all electronic voting machines used in the County with progress reports to the general public regarding this program.

Finding VI

Absentee ballots are unsecured when outside the physical control of the Registrar's office.

Recommendation VI

The Registrar of Voters should address the lack of security for absentee ballots by devising methods to insure their security and to provide verification of receipt to the voter.

Finding VII

To prevent electronic tampering from the outside, the individual voting machines and the entire system now stand alone electronically. No part of the system is ever connected to the Internet or similar electronic pathway for the transmission of information.

Recommendation VII

This policy should be continued.

Finding VIII

The Registrar has been extremely conscientious, not only in working with citizens in the selection and ongoing operations of the electronic voting machines, but also in educating the general public in this new system of voting.

Recommendation VIII

The Registrar should continue to make use of citizen advisors as the system moves to a printed paper trail and during other refinements of the voting process.

Finding IX

Paper or absentee ballots are not provided at polling places as an alternative means of voting.

Recommendation IX

Paper ballots should be provided at each polling place in case all the machines are taken out of service or for voters who cannot or will not use the electronic machines.

PASSED and **ADOPTED** by the Santa Clara County Civil Grand Jury on this 6th day of May 2004.

_____

Richard H. Woodward
Foreperson

References

Documents

Ad Hoc Touch Screen Task Force, California, Report to Secretary of State, July 2, 2003.

Analysis of an Electronic Voting System, Department of Computer Sciences, Rice University.

Analysis of an Electronic Voting System, John Hopkins Information Security Technical Report TR-2003-19.

Election Reform and Electronic Voting Systems—Analysis of Security Issues, Congressional Research Service, November 4, 2003.

News articles from local and national newspapers and magazines, 2003-2004.

Report on security flaws in electronic voting machines, Ohio Secretary of State.

Santa Clara County Registrar of Voters documents:

- Absentee Canvass Procedures
- Election Security and Procedures Manual
- Electronic Voting Machines Logic and Accuracy Test Procedures
- Electronic Voting Machines Procedures for the Return Center
- Media, Outreach & Voter Education Committee Summary & Calendar
- Polling Place List for November 2003 Election

Santa Clara County Registrar of Voters press releases:

- County Awards Electronic Voting Contract to Sequoia
- County of Santa Clara Gears up for Electronic Voting
- Staff Recommends Sequoia Voting Systems
- Supervisors Approve Citizens Oversight Committee for Electronic Voting
- Supervisors Select Electronic Voting Machines—Want "Paper Record" Study
- Supervisors Vote for Further Deliberation on Electronic Voting Machines

Santa Clara County Registrar of Voters website:

- Analysis of budget increases for Electronic Voting Machines

Secretary of State News Release dated April 30, 2004.

Sequoia Voting Systems web site articles:

- Santa Clara County ranks Sequoia Voting Systems
- Sequoia Discusses Safeguards of Electronic Voting

Series of E-Mail reports on electronic voting from senior engineer, software company.

The Case of the Diebold FTP Site, University of Iowa, Department of Computer Sciences.

"Watching the Count" clips from the Progressive Review, August 2003.

Who Counts the Votes?, *Southern Exposure.*

Interviews & Visits

Registrar of Voters for Santa Clara County, August 1, 2003, Feb. 9, 2004 and May 3, 2004.

Tour of Registrar of Voters facilities, October 23, 2003.

Visit to Registrar of Voters for debriefing from field operations, December 10, 2003.

Visit to Registrar of Voters office during ballot counting, November 4, 2003.

Visits to polling places to check security, November 3, 2003, March 1, 2004.

Visits to polling places to view voting, November 4, 2003, March 2, 2004.

Presentation

Presentation by private expert on electronic voting, December 3, 2003.