Verified Voting Foundation

Verified Voting Foundation
454 Shotwell Street
San Francisco, CA 94110

Phone +1 415 695-0543
Fax +1 928 244-2347

Electronic Voting Systems

A Report for the National Research Council by
David Dill and Will Doherty
Verified Voting Foundation

November 22, 2004

Chapter 1

Introduction

The Verified Voting Foundation (VVF) was founded in 1993 by Stanford University Computer Science Professor David Dill[i] for the purpose of ensuring transparency and reliability of voting technology used in elections in the United States. As a nonprofit, nonpartisan voter protection organization, VVF has initiated various projects aimed at achieving these goals, including TechWatch[ii], a program for involving technologists in election protection activities and, in cooperation with Computer Professionals for Social Responsibility, the Election Incident Reporting System[iii] (EIRS), a web-based software application that made it possible for the Election Protection Coalition[iv] to track and respond to problems with elections starting with the Florida primary election on August 31, 2004. The Verified Voting Foundation also partnered with the Brennan Center at New York University, the Leadership Conference for Civil Rights, and the Center for American Progress to administer an Election Practices Report Card[v] to 100 counties using electronic voting technology in September-October 2004. Our leadership and participation in these and other projects informs this report.

Even our preliminary analysis of the still not fully compiled set of electronic voting incidents reported so far on the Election Protection Hotline and Election Incident Reporting System during Election 2004 suggests a substantial base of questions about the functioning of electronic voting machines in live election situations.[vi]

To cite a small sample of notable examples--

- Carteret County, North Carolina: a Unilect PATRIOT electronic voting machine with a reported storage capacity of 10,500 votes lost approximately 4,530 votes in early voting because the machine was set at a capacity of 3,005 votes and failed to tally the remainder of the 7,537 votes cast.[vii] There is no way to recover these lost votes; the only option to make sure those North Carolina voters could vote would be to run the election over again.

- New Orleans, Louisiana: 80+ reports with 42 reports of total breakdowns, with long lines and voters turned away from polling places, for example, "All voters have been unable to vote on touchscreen machines. There are no paper ballots. The precinct official tried to call the Sect'y of State's office for guidance but could not get through. (Not clear if county officials were contacted). Precinct officials don't know what to do."[viii]

- Dauphin, Mercer, and Philadelphia Counties, Pennsylvania: Dauphin County had five reports of machine power failure and faulty machine operation. "There were only 2 machines available for the largest precinct in the area at 101 18th Street, but only one of the machines worked."[ix] Mercer County had 15 reports of catastrophic machine failure.[x] All voter machines were down, and makeshift paper ballots were provided but in some cases were not secured. Philadelphia reports included 28 complaints of misrecording of votes as well as 28 reports of total breakdowns.[xi]

- Broward, Miami-Dade, and Palm Beach Counties, Florida: Broward County reported multiple miscrecordings of votes, as in this report: "At review screen, selection changed from Kerry to Bush 'before my eyes' as voter pushed red button just before. Voter filed complaint with Kerry lawyer in polling place and told poll worker of problem, who said, 'nothing could be done,'" while another report indicated a Bush vote displaying as Kerry and yet another mentioned a machine that would only take votes in Spanish.[xii] Miami had a "predominantly African-American precinct; computer crash with problem screens on one bank of machines daisy-chained into one another. Technician considered unplugging machines, told not to by supervisor or votes would be lost. Technician said that batteries had been compromised," as well as this report: "Voter has been in line for over 3 hrs. 5 machines (normally are 16-18 machines). Pulled 3 machines - not working - originally 8 machines."[xiii] Palm Beach reports included this one: "At precinct, they gave a plastic card to put in machine. Then you had to wait in line and the line was long so many of the cards were expiring and so you couldn't vote. They then forced you to get back in line. Many people left because they were frustrated," as well as lots of misrecording problems and a case where a blind person could not vote unassisted because the audio device was malfunctioning.[xiv]

- Franklin and Mahoning Counties, Ohio: Franklin County reports long lines and voters leaving due to machine breakdowns with reports like "3 hour wait in line to vote. 5 machines working before; only 3 working now." [xv] Mahoning County reported machine breakdowns, misrecordings, and this problem with disabled access: "When a handicapped voter can't get inside the polls, the machine is brought out to the voter. But because all the machines are connected, everything inside stops until the handicapped voter is done voting." [xvi]

- Bernalillo County, New Mexico: reports of candidates or races not listed, not selectable, or deselecting on the electronic voting machines, for example, "Machine registered full slate of votes for the wrong party. Voter had to go back and manually change each category." [xvii]

Among the nearly 900 electronic voting incidents reported, the variety of types of failures, malfunctions, and errors across almost all vendors' electronic voting machine models and across most jurisdictions where electronic voting machines are deployed suggest a significant need for further inquiry.[xviii] These incidents impacted at a minimum tens or hundreds of thousands of voters and, because many incidents go unreported, may represent only the tip of the iceberg of all actual incidents that occurred.

The electronic voting as well as other types of incident reports from EIRS provide an excellent opportunity for dialog among election administrators, policymakers, voting technology providers, media professionals, and the public in improving election processes, technologies, and regulation.

This type of inquiry is important because it impacts the ability of voters to cast their votes and have them counted as intended, the very foundation of a democratic system.

Chapter 2

Questions Raised by Electronic Voting

The use of electronic voting technology in U.S. elections raises a variety of questions of interest to policymakers and the voting public in the following areas: Election Administration, Election Transparency, Election Security, Audits and Recounts, Voting Technology Standards, Qualification, and Certification, Voting Technology Testing, Voter Registration and Provisional Ballots, and Voter Privacy and Accessibility.

Election Administration

- Some regulatory agencies require incident reports and routinely investigate potential safety problems. Should there be a mandatory or voluntary incident reporting system for election problems? If so, what sort of problems should be reported, at what level of detail? How should reports be investigated? What agency or agencies should have the responsibility of collecting the reports and investigating them?

- There is a need for systematic analysis of the types of failures that can occur, how they affect voters, and what measures can be put in place to minimize the impact on voters. For example, many voters throughout the country were asked to vote on paper provisional ballots when electronic voting equipment failed. But the consequences of treating these votes as provisional are unclear, and in some cases, provisional ballots ran out.

- What is an adequate level of poll worker training and polling place staffing? How does the answer to this question vary depending on the election technology in use? In particular, what are the explanations of the long lines experienced in many parts of the country on Nov. 2, and what can be done to prevent these problems in the future?

- What are appropriate policies to ensure the integrity of polling place procedures? Should there be policies to make sure that there are at least two clearly-identifiable poll workers on duty at all times? Should there be poll workers representing both parties at each polling place and central tabulation facility? How should authorized personnel be identified at polling places and election offices? Who should be allowed to handle ballots (in particular, how should access to ballots and counting equipment by private consultants and employees of voting machine companies be controlled)?

- How does the use of electronic voting impact poll opening, poll closing, and the accumulation of vote counts at central tabulation facilities?

- What is the best way for election administrators to determine a sufficient number of paper ballots to keep on hand at each polling place to ensure no voter is turned away due to system failures?

- Should election administrators permit no vendor technicians, nor any other vendor employees, to handle ballots (other than their own), open polls, close polls, handle memory cards or cartridges, or perform any other activity critical to the election process?

Election Transparency

Election transparency is what enables observers from the political parties, media, NGOs, and public to observe the conduct of the election and check for themselves that results are accurate.

Currently, insiders have a major information advantage of members of the public, whether those insiders are voting equipment vendors or election officials. There are many questions about what we can do to increase the transparency of elections..

- What election data should be made publicly available, and when should it be available? Should data be released in a standard form to make it more comprehensible and easier to analyze? Should absentee votes be associated with the precincts in which the voters are registered? How can we ensure that the reports are as accurate as possible? Should electronic ballot images be published when possible?

- What concerns work against the release of more election data? Possible concerns include: information about exploitable security vulnerabilities, and information that may compromise the privacy of voters or facilitate vote buying.

- How do various voting technologies support or dscourage greater transparency in elections? For example, digital recording electronic (DRE) e-voting machines hide much of the voting process inside the machines where no one can observe it; on the other hand, many optical scan systems do not have the capability to acquire electronic ballot images, which makes this data difficult and expensive to obtain.

- Should incident reports be made available to news media and the public (redacting only when necessary to protect voter privacy or prevent exploitation of security flaws exposed by the incident)?

- How does voting technology affect the ability for candidates to obtain meaningful recounts? This question has been raised about DREs, since recounts cannot detect electronic ballot copies that have been corrupted accidentally or deliberately by the voting system. However, even leaving the question of paper ballots aside, there are open questions about whether candidates can access the electronic audit logs and ballot images they might need to resolve questions about the election (for example, in Soubirous v. County of Riverside[xix], a candidate was denied access to backup electronic records and audit logs that could have been used to resolve questions about the integrity of electronic records in the central election management system).

- How does use of electronic voting impact the posting of vote totals and polling place statistics (on absentee and provisional votes, over- and under-votes, spoiled ballots, and ballots issued or voters signed in) for public review at each polling place at close of polls as well as accumulation of vote counts at central tabulation facilities? Should election administrators print polling place totals at the polling place *before connecting any electronic communications* out of the polling place?

- How would the use of open source software in electronic voting systems impact public confidence in election results?

- What access should be granted to those who wish to observe the conduct of the election? The ability to watch critical aspects of the election, such as pre-election equipment testing, polling place procedures, and the counting and recount of votes, is an essential of election transparency. However, in many states, it is difficult or impossible for non-partisan observers to fill these roles.

- How can election processes be made more observable? More access can be granted by changes in procedures, such as by conducting central tabulation procedures and recounts in full view of the public. But there may be opportunities for innovative use of technology as well. For example, San Mateo County Registrar of Voters Warren Slocum used a “web-cam” to broadcast the testing of the machines in his warehouse over the internet.

- How can we ensure that vote totals from the precincts accurately appear in the central tabulation? It has been observed that vote totals in election management systems can be changed easily, especially by those with authorized access to the systems.

- Should election administrators document and publish the rights of observers at polling places and at the tabulating center as well as the obligations of election officials to inform and disclose election administration activities?

Election Security

- What is the appropriate threat model for voting systems, and how do those models change with technology? Who are the possible attackers, and what would be their level of motivation and sophistication, and what resources might they bring to bear?

- Do effective means exist to establish the integrity of computerized election equipment by testing or inspection? In particular, is it feasible to detect potential malicious behavior of voting system software and hardware? If so, what are the techniques, and what are the costs of applying them?

- How can we make sure that election offices have received expert advice in computer security and other security issues? What sort of expertise is required? How do election officials know that the experts they retain are properly qualified? How do we make sure that any problems identified are addressed?

- How should election officials administering jurisdictions with electronic voting technology control access to the various components of electronic voting equipment used in polling places and central tabulation facilities, including access by voting technology vendor personnel?

- How does the use of voter-verified paper ballots in electronic voting systems impact electronic voting system security?

- How would the use of open source software in electronic voting systems impact electronic voting system security?

- Should election administrators seal (with numbered tamper-evident seals) and log all physical (paper and electronic) polling place records; then check and log seal numbers when received from polling place?

- Should election administrators use logged, numbered, tamper-evident seals to prevent use of the voting machines between the time they pass pre-election testing and the poll-opening process?

- Should election administrators make sure each machine has a unique secure key/password?

- Should election administrators require that all persons entering or leaving the tabulating center provide legal identification and sign in and out on a public log (citing: elections employee, temporary employee, contractor, or visitor)?

- Should election administrators require two or more poll workers of opposing parties accompany ballots to the counting facility?

- What remedies should be in place in the case of violation of security procedures and who should determine and enforce them?

Audits and Recounts

- How does the use of electronic voting impact the election audit process and how does this vary by jurisdiction?
- How does the use of electronic voting impact the election recount process and how does this vary by jurisdiction?
- If voter-verified paper ballots are used along with electronic voting machines, which should be the ballot of record -- paper or electronic – and under which circumstances?
- If voter-verified paper ballots are used in an audit of an electronic voting system, what percentage of the polling places, chosen at random, is sufficient to provide a good audit of the system? Who should be responsible for choosing the polling places for the audit and by what mechanism?
- Should election administrators' documented Election Day procedures require reconciling the number of voters who signed the poll book (or roster) with the number of votes cast in that polling place?
- Should election administrators routinely compare paper records printed at the polling place when the polls close with electronic records transmitted and/or hand carried from the polling place?
- Should election administrators routinely inspect audit logs from voting machines and the election management system to reconcile the number of ballots cast with votes reported, to check when polls opened and closed, and to check for any unusual events?

- Should election administrators routinely log and audit chain-of-custody records for voting machines, blank and voted ballots and physical copies of electronic records, including seal numbers and who had custody when?

- Should election administrators perform “parallel testing” during Election Day, simulating a real election (poll opening, voting, and poll closing) on a few machines randomly selected from polling places on Election Day?

- What happens if audit mechanisms show a discrepancy? What if parallel testing shows flawed software? Should there be a set of specified remedies in place for such eventualities, and who should establish them?

Voting Technology Standards, Qualification, and Certification

- Should there be minimum federal standards for electronic voting technology used in elections and, if so, what should these federal standards be? Should they be voluntary, dependent on use of federal funding, or mandatory, and why?

- What should be the requirements for organizations responsible for qualifying and/or certifying electronic voting technology for use in elections?

- Should voting technology vendors, the federal government, or some other sources fund the federal qualifications of their products, and what impact does the source of funding have on the results of federal qualification testing?

- Should the results of federal qualification testing be kept secret or made public as part of the federal qualification process?

- Should states perform separate certifications of voting technology in concert with federal qualifications?

- Should the results of any state certification testing be kept secret or made public as part of a state certification process?
- In compliance with which standard or standards should electronic voting technology be qualified or certified?
- How should electronic voting standards be developed and updated and by whom?

Voting Technology Testing

- Should election administrators test all machines using automatic self-test scripts executed on the machines?
- Should election administrators test audio and ot her accessibility interfaces?
- Should election administrators test all ballot positions in all languages?
- Should election administrators select at random and test intensively by hand some machines in a realistically simulated election (realistic votes, hand testers simulate errors and change votes, clock set to Election Day)?
- Should election administrators select at random and test intensively some machines in "parallel testing" during Election Day? And during early voting, if any?
- Should election administrators explain all pre-election testing to those who have come to observe the testing procedures, all of which are open to members of the public?

Voter Registration and Provisional Ballots

- Should election administrators check county-wide voter registration databases to assist voters not listed in the polling place's voting rolls in finding the correct polling place?

- Should election administrators inform all voters not listed in the polling place's voting rolls of their right to vote on a provisional ballot and permit them to do so?

Voter Privacy and Accessibility

- Should election administrators arrange screens, booths, and equipment in each polling place to ensure voter privacy?
- Should election administrators make sure a bi-partisan group with representation from relevant language minority and disabled community organizations has reviewed polling locations and layouts for accessibility?
- Should election administrators make sure all polling places meet ADA and HAVA definitions of accessibility?
- Should election administrators make sure handicapped voters do not need to request special accommodation in advance?
- Should election administrators make sure members of the public, including persons of representative ages and ethnicity, test ballot layouts to reduce voter confusion due to wording, layout, iconography, or machine configuration?

Chapter

3

Answers to Electronic Voting Concerns

Although the Verified Voting Foundation has a number of recommendations related to the questions about electronic voting raised above, time constraints prevent us from including our specific recommendations in this report. We are looking forward to participation in further research and discussions toward improving elections process, technology, and regulation, especially as it related to electronic voting.

Chapter
4

Electronic Voting Problems Reported in 2004

Voters, voter protection volunteers, attorneys, technologists, and media professionals, reported the following types of problems with electronic voting technology to the Election Protection Hotline and thus into the Election Incident Reporting System during the 2004 election cycle.[xx]

- Machine breakdown (total malfunction, sometimes entire polling places, power/battery failures, machines locked, long lines, voters turned away)
- Misrecording (Kerry recorded as Bush and occasionally vice-versa, likely touchscreen calibration problems)
- Vote switched
- Overcounts and undercounts
- Wrong ballot or race/candidate/party slate missing or not working, no write-ins
- Prefilled ballot choice
- Straight ticket sticking
- Unintended deselections
- Forced votes to complete ballot
- Indicates "challenged ballot"
- Not responding to human touch, just pencil eraser
- Disabled accommodation disables other machines at polling place
- Non-"accessible" voting machine, audio component not working
- Premature casting
- Overwritten votes (prior uncast)
- Switched language (English to Spanish), or Spanish-only
- Vote card times out, rejected, stuck, not reset, or cancels ballot
- Claims vote cast after card removed

- Blank screen / screen goes dark
- Missing or poor distribution of machines
- Audio offers only one candidate
- No paper ballot alternative
- Paper ballots treated as provisional
- Told to use demo machine
- Inadequate poll worker training
- Not zeroed out at beginning of day
- Security seals broken
- Infrared port available
- Cascading error in machine cluster

Chapter 4

Reference Citations

[i] David Dill biographical sketch at http://verifiedvoting.org/article.php?id=5008#dill .

[ii] TechWatch project description at http://www.verifiedvoting.org/techwatch/ .

[iii] Election Incident Reporting System project description at http://www.verifiedvoting.org/eirs/ .

[iv] Election Protection Coalition member organizations list at http://www.electionprotection2004.org/coalition.htm .

[v] To see election administrator responses to the Election Practices Report Card, go to http://www.verifiedvoting.org/verifier/index.php?state=&topic_string=1018 and click on any colored state, then any colored county or equivalent jurisdiction to view the responses below the map..

[vi] Election Verification Project statement announcing initial EIRS results on e-voting at http://www.verifiedvoting.org/article.php?id=5302 .

[vii] Carteret County, North Carolina, incident, case 51781 in the Election Incident Reporting System at https://voteprotect.org/epc/index.php?display=EIRBrowseIncidents&cases=51781 , with reporting from newspapers listed at http://verifiedvoting.org/search.php?q=Carteret .

[viii] New Orleans, Louisiana, case 32335 in the Election Incident Reporting System at https://voteprotect.org/epc/index.php?display=EIRBrowseIncidents&cases=32335 .

[ix] Dauphin County, Pennsylvania, cases such as 50206, 42629, and 42026 in the Election Incident Reporting System at https://voteprotect.org/epc/index.php?display=EIRBrowseIncidents&cases=50206,42629,42026 .

[x] Mercer County, Pennsylvania, cases such as 34369, 33679, and 36729 in the Election Incident Reporting System at https://voteprotect.org/epc/index.php?display=EIRBrowseIncidents&cases=34369,%2033679,36729 .

[xi] Philadelphia County, Pennsylvania, cases such as 29076, 31326, and 30095 in the Election Incident Reporting System at https://voteprotect.org/epc/index.php?display=EIRBrowseIncidents&cases=29076,31326,30095 .

[xii] Broward County, Florida, cases such as 55055, 48034, and 45884 in the Election Incident Reporting System at https://voteprotect.org/epc/index.php?display=EIRBrowseIncidents&cases=55055,48034,45884 .

[xiii] Miami-Dade County, Florida, cases such as 42378, 32122, and 32038 in the Election Incident Reporting System at https://voteprotect.org/epc/index.php?display=EIRBrowseIncidents&cases=42378,32122,32038 .

[xiv] Palm Beach County, Florida, cases such as 35503, 31377, and 34517 in the Election Incident Reporting System at https://voteprotect.org/epc/index.php?display=EIRBrowseIncidents&cases=35503,31377,34517 .

[xv] Franklin County, Ohio, cases such as 32718, 30943, and 30287 in the Election Incident Reporting System at https://voteprotect.org/epc/index.php?display=EIRBrowseIncidents&cases=32718,30943,30287 .

[xvi] Mahoning County, Ohio, cases such as 35882, 35862, and 38279 in the Election Incident Reporting System at https://voteprotect.org/epc/index.php?display=EIRBrowseIncidents&cases=35882,35862,38279 .

[xvii] Bernalillo County, New Mexico, cases such as 47355, 36750, and 34353 in the Election Incident Reporting System at https://voteprotect.org/epc/index.php?display=EIRBrowseIncidents&cases=47355,36750,34353 .

[xviii] Election Verification Project press conference handout available at http://verifiedvoting.org/article.php?id=5331 .

[xix] Information about the Soubirous v. Riverside County case is available in the California section of the Verified Voting Foundation's Litigation web page at http://www.verifiedvoting.org/article.php?list=type&type=15 .

[xx] Election Verification Project press conference handout available at http://verifiedvoting.org/article.php?id=5331 and case 51781 in Election Incident Reporting System at https://voteprotect.org/epc/index.php?display=EIRBrowseIncidents&cases=51781 .