

MINUTES OF THE SENATE ELECTIONS AND LOCAL GOVERNMENT

The meeting was called to order by Chairman Tim Huelskamp at 1:36 P.M. on January 27, 2005 in Room 423-S of the Capitol.

All members were present.

Committee staff present: Martha Dorsey, Kansas Legislative Research Department
Mike Heim, Kansas Legislative Research Department
Ken Wilke, Revisor of Statutes
Janet Engel, Committee Secretary

Conferees appearing before the committee:

Brad Bryant, Deputy Assistant Secretary of State
Brian Newby, Johnson County Election Commissioner

Others attending: See attached list.

Bill Introductions

Senator Huelskamp received a request from Representative Gilstrap to introduce a bill changing timing for cities to file quarterly reports from 30 to 45 days. It was moved by Senator Wilson and seconded by Senator Reitz that the committee introduce the requested bill. Motion carried.

Informational Session

Brad Bryant provided a report, "Discussion on Electronic Voting" (Attachment 1). Details and exhibits were provided including the certification process, types of equipment, security, and 2006 procurement under HAVA. He fielded questions from the committee with the assistance of Anthony Fadale and Michael Byington who were in the audience.

Brian Newby provided a report, "Voting Systems Overview" (Attachment 2). It covered operations, security, and accountability as used in Johnson County. He also showed electronic voting machines currently used in Johnson County. The included features geared toward physically handicapped voters. He fielded questions from the committee.

Other Business

Senator O'Connor reported that Senator Brownlee asked the committee to have a bill drafted related to advance ballot requests that do not carry the correct signatures. It was moved by Senator Wilson and seconded by Senator Reitz to ask that a committee bill be drafted. Motion carried.

Closing

Time having run out, the meeting was adjourned at 2:30 p.m. Many committee members stayed to look at and/or try the voting machines on display.

Senate Elections & Local Government Committee
 Daily, 1:30 - 2:30 p.m. Room 423-S
 Sen Tim Huelskamp, Chair

Guest List for January 27, 2005
 Please sign in

Name	Representing
Jesse Borjon	KSOS
Mike Stewart	KSOS
BRYAN A. CASKEY	KSOS
Jennifer Landell	Jolo. Election
DEBORAH TYRREL	JOCO ELECTIONS
BRIAN NEWBY	JOCO ELECTION OFFICE
Veronica Hoskinson	Sen. O'Connor
Sarah Strik	SEN. FRANCISCO
Julia Gilmore Gaughan	DRC
Anthony A. Fedale	ADA/ Admin
Michael Byington	KS. Assn F/T Blind + Vis Impaired
Sharon Joseph	KS ADA/PT
Brad Bryant	Sec. of State
Brian Henson	Sec of State

RON THORNBURGH
Secretary of State



Memorial Hall, 1st Floor
120 S.W. 10th Avenue
Topeka, KS 66612-1594
(785)296-4564

STATE OF KANSAS
Senate Committee on Elections and Local Government

Discussion on Electronic Voting

Brad Bryant, Deputy Assistant Secretary of State
Elections and Legislative Matters

January 27, 2005

1. Certification process

Secretary of State certification
Federal Election Commission voluntary standards
Tested and qualified by independent testing authority approved by National Association
of State Election Directors
Federal law
Kansas law

2. Types of equipment used

105 counties
3 DRE (direct recording electronic)
1 combination DRE and optical scan
82 optical scan
19 hand counted paper ballots

3. Security

Policy developed in 2004 and adopted in May, 2004 by the Kansas County Clerks and
Election Officials Association
Adds security, promotes consistency of procedures

4. 2006 procurement under HAVA

One fully accessible, ADA compliant device per polling place
HAVA does not require replacement of all existing voting equipment, and HAVA
funding does not support it

(i) establishing a voter education program specific to that voting system that notifies each voter of the effect of casting multiple votes for an office; and

(ii) providing the voter with instructions on how to correct the ballot before it is cast and counted (including instructions on how to correct the error through the issuance of a replacement ballot if the voter was otherwise unable to change the ballot or correct any error).

(C) The voting system shall ensure that any notification required under this paragraph preserves the privacy of the voter and the confidentiality of the ballot.

(2) AUDIT CAPACITY.—

(A) IN GENERAL.—The voting system shall produce a record with an audit capacity for such system.

(B) MANUAL AUDIT CAPACITY.—

(i) The voting system shall produce a permanent paper record with a manual audit capacity for such system.

(ii) The voting system shall provide the voter with an opportunity to change the ballot or correct any error before the permanent paper record is produced.

(iii) The paper record produced under subparagraph (A) shall be available as an official record for any recount conducted with respect to any election in which the system is used.

(3) ACCESSIBILITY FOR INDIVIDUALS WITH DISABILITIES.—

The voting system shall—

(A) be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters;

(B) satisfy the requirement of subparagraph (A) through the use of at least one direct recording electronic voting system or other voting system equipped for individuals with disabilities at each polling place; and

(C) if purchased with funds made available under title II on or after January 1, 2007, meet the voting system standards for disability access (as outlined in this paragraph).

(4) ALTERNATIVE LANGUAGE ACCESSIBILITY.—The voting system shall provide alternative language accessibility pursuant to the requirements of section 203 of the Voting Rights Act of 1965 (42 U.S.C. 1973aa-1a).

(5) ERROR RATES.—The error rate of the voting system in counting ballots (determined by taking into account only those errors which are attributable to the voting system and not attributable to an act of the voter) shall comply with the error rate standards established under section 3.2.1 of the voting systems standards issued by the Federal Election Commission which are in effect on the date of the enactment of this Act.

(6) UNIFORM DEFINITION OF WHAT CONSTITUTES A VOTE.—Each State shall adopt uniform and nondiscriminatory standards that define what constitutes a vote and what will be

Voting Systems in Kansas Counties

Allen	Opti scan ^{2p}	20 Paper Ballots 82 Optical Scan Ballots 3 Electronic Voting	Norton	Paper
Anderson	Opti scan ^{1p}		Osage	Opti scan ^{2p}
Atchison	Opti scan ^{2c}		Osborne	Opti scan ^{2c}
Barber	Opti scan ^{1p}		Ottawa	Opti scan ^{1p}
Barton	Opti scan ^{2c}		Pawnee	Opti scan ^{2c}
Bourbon	Opti scan ^{2c}		Phillips	Opti scan ^{2c}
Brown	Opti scan ^{1p}	Hamilton	Pottawatomie	Opti scan ^{2c}
Butler	Electronic ³	Harper	Pratt	Opti scan ^{1c}
Chase	Opti scan ^{1p}	Harvey	Rawlins	Paper
Chautauqua	Paper	Haskell	Reno	Opti scan ^{1p}
Cherokee	Opti scan ^{2c}	Hodgeman	Republic	Paper
Cheyenne	Paper	Jackson	Rice	Opti scan ^{2c}
Clark	Opti scan ^{1p}	Jefferson	Riley	Opti scan ^{2c}
Clay	Opti scan ^{2c}	Jewell	Rooks	Opti scan ^{1p}
Cloud	Opti scan ^{2c}	Johnson	Rush	Paper
Coffey	Opti scan ^{2c}	Kearny	Russell	Opti scan ^{2c}
Comanche	Paper	Kingman	Saline	Opti scan ^{2c}
Cowley	Opti scan ^{2c}	Kiowa	Scott	Opti scan ^{2c}
Crawford	Opti scan ^{2c}	Labette	Sedgwick	Electronic ³
Decatur	Paper	Lane	Seward	Opti scan ^{1p}
Dickinson	Opti scan ^{2c}	Leavenworth	Shawnee	Opti scan ^{1p}
Doniphan	Opti scan ^{1p}	Lincoln	Sheridan	Opti scan ^{2c}
Douglas	Opti scan ^{2c}	Linn	Sherman	Opti scan ^{2c}
Edwards	Opti scan ^{2c}	Logan	Smith	Opti scan ^{2c}
Elk	Paper	Lyon	Stafford	Opti scan ^{2c}
Ellis	Opti scan ^{2c}	Marion	Stanton	Opti scan ^{1c}
Ellsworth	Opti scan ^{2c}	Marshall	Stevens	Opti scan ^{2p}
Finney	Opti scan ^{2c}	McPherson	Sumner	Opti scan ^{2c}
Ford	Opti scan ^{2c}	Meade	Thomas	Opti scan ^{2p}
Franklin	Opti scan ^{2c}	Miami	Trego	Opti scan ^{2c}
Geary	Opti scan ^{2c}	Mitchell	Wabaunsee	Opti scan ^{1c}
Gove	Paper	Montgomery	Wallace	Opti scan ^{1p}
Graham	Paper	Morris	Washington	Paper
Grant	Opti scan ^{1p}	Morton	Wichita	Paper
Gray	Opti scan ^{1c}	Neosho	Wilson	Opti scan ^{2c}
Greeley	Opti scan ^{1p}	Nemaha	Woodson	Paper
Greenwood	Opti scan ^{2p}	Ness	Wyandotte	Opti scan ^{1p}

1 Diebold AccuVote (28) 2 ES&S (53) 3 MicroVote 4 Diebold AccuTouch (1)
P-Precinct Scan (30) C-Central Scan (52)

INTRODUCTION

A. Overview of Voting Systems

B. Six Components of Voting System Security

1. Access to the system
2. Transmitting data
3. Testing voting equipment
4. Polling place security
5. Equipment storage
6. Voting equipment certification process

INTRODUCTION

Security of any computer-based system requires a combination of three factors. First, the computer must provide audit data that is sufficient to track the sequence of events that occur on the system and, to the extent possible, identify the person(s) that initiated the events. Next, there must be well defined and strictly enforced policies and procedures that control who can access the system, the circumstances under which they can access the system, and the functions that they are allowed to perform on the system. Finally, there must be physical security in place such as fences, doors and locks that control and limit access to the equipment. It is recommended that each county adopt the following policy and its six components, but each may have different procedures for adhering to the policy. Kansas counties currently use DRE, optical scan and paper ballots to conduct elections, and each requires different procedures to implement the security policy.

A. Overview of voting systems

Direct recording electronic (DRE): A standard personal computer running an executable software module is used to define the election, enter the candidates and questions, and format the ballots for the voting devices. This computer also accumulates the votes after the polls close and prints various reports and audits. Three Kansas counties currently use DRE systems, and a fourth uses a combination of DRE and optical scan.

Optical scan: A paper ballot is used to cast a vote and is then fed through a scanner. The device reads the voter's marks on the ballot, and tabulates number of votes cast for each candidate or question. Eighty-one Kansas counties currently use optical scan systems.

Paper ballot: Votes are recorded on paper ballots and counted by hand. Twenty-one Kansas counties currently use paper ballots.

B. Six components of voting system security

1. Access to the system

- stand-alone system
- no network connection
- no modem
- only operating system and voting software loaded
- controlled access with authorized users

The computer-based voting system should not be connected to any network and it should not have a modem. If it does have a modem, it shouldn't be connected to the Internet. The computer should have only the operating system and voting software loaded. Additional applications could jeopardize system security.

If the computer has no outside connections, it can only be accessed by county election staff or other authorized persons. Any such system should also have password requirements. There should be strict procedures that control who has access to the election system, when they can access the system, what components they can access, and what functions they are allowed to perform.

The computer portion of the election system contains features that facilitate overall security of the election system. Primary among these features is a comprehensive set of audit data. For transactions that occur on the system, a record is made of the nature of the transaction, the time of the transaction, and the person that initiated the transaction. This record is written to an audit log to allow the sequence of events surrounding the incident to be reconstructed.

A security program, similar to a virus detector program, should be run against the operating system and the election tabulation software before beginning the definition of an election to verify that the code has not been altered. This program should be repeated after the close of the election to verify that the code did not change during the election.

Permanent storage of media containing certified application programs should be within a secure, fireproof location such as a safe. Additional backup copies of application programs and media containing election data should be created and stored securely off site.

2. Transmitting data

- No data transmission by modem – from polling place to election office or from election office to state.

It is important that results from elections not be sent from polling places to election offices via modem, network, phone line, cable, or any other electronic form of file transmission. The same applies when sending results from the county election office to the Secretary of State's office. Results should be sent by fax, phone or by inputting the results in the SOS database directly using an IP address and/or using the state's secure Public Key Infrastructure (PKI) system.

3. Testing voting equipment

- public test five days prior to election
- test before public test
- test after canvass
- print zero totals
- end of day totals

Voting equipment should be tested when it is first received from the vendor. Tests should cover all functions that will be necessary to conduct an election. Prior to use in an election, each voting machine should undergo system diagnostics to ensure proper operation of certified components. A checklist confirms the outcome of acceptability. Any component failure should be logged and repairs to equipment performed as soon as practical.

4. Polling place security

- hardware security
- software security
- poll worker procedures

There are many polling places in Kansas that simply do not provide an ideal physical security environment. For instance, church lobbies, school gymnasiums and other places may not always be locked or secured. The county election officer should, to the extent possible, designate polling sites that afford the necessary security features and should maximize the use of whatever security features exist.

The memory cards in each touch screen voting station should be stored within a locked compartment. The supervising judge should be the only person with a key to this compartment. The memory cards and/or ballots from each voting location are transported from the voting location to the county elections office by a sworn election official or a sworn law enforcement officer.

The area of the voting location that contains the voting stations is secure. A voter is not allowed to enter this area until a voting station is available for his or her use. No person other than a voter, a person assisting a voter, or a poll worker may enter this area.

Voting machine protective counters should be observed and recorded with a date of record. Voting machines and ballot boxes should be sealed before delivery to polling place locations. Seals should be tamperproof and serialized with numbers. Logging of machine serial number, seal number and designated voting location is an essential part of the audit trail.

Equipment delivery:

Voting equipment delivery to polling place locations should be conducted with the same degree of control as applied to storage. A delivery person or company should continue the audit trail for the election officer. Documentation and daily reporting are essential.

- The delivery person or company, or in some cases the supervising judge, should provide documentation containing voting machine numbers, seal numbers and identification for each voting location where equipment has been delivered.
- A list of persons involved in equipment delivery should be maintained by the county election officer.
- Voting machines should remain locked and stored in a secure location. Multiple voting machines should be secured together by a keyed or combination lock and a single cable or chain. Additional supplies delivered with machines should be secured with the same cable or chain.
- Polling places should be in locked buildings or locations that are capable of monitoring secure storage of voting equipment.

Election worker security awareness and requirements:

All election judges are responsible for maintaining the security of the polling place, the integrity of the vote and the protection of voting equipment and supplies. Judges must be vigilant throughout election day and be aware of who is in the polling room. Frequent monitoring of voting machines and securing voting supplies ensures that any malicious attempt to compromise the accurate gathering and reporting of the vote is unsuccessful. The following steps should be taken to ensure that the voting equipment and the voting process are secure at all times in every precinct:

Supervising judges:

- Inspect voting machines for physical damage while setting up or closing units and record on maintenance log. Examples: damaged or broken lid hinges, cracked cases, and damage to equipment inside case.

- Control and secure keys to all voting machines.
- Assure that the election media slot (memory cartridge slot area) on every voting machine is locked.
- Report any suspicious activity in or around voting machines to the county election officer and call 911 if immediate help is required.

5. Equipment storage

- election computers should be kept in locked offices
- physical security during non-election times
- protective seals
- limited access

The first line of defense in any system is physical security. When not in use, all election equipment should be stored in a locked room. Access to the room should be limited to election officials and authorized county officials or technicians. A paper activity log should be maintained to record date, time, staff person, and reason for entering the secured computer room. A video camera is *recommended* to be installed in the locked office to monitor activity. All voting machine keys, voter cards, and storage media should be secured in a controlled access room. Staff should maintain a detailed inventory control of these supplies:

6. Voting equipment certification process

Kansas participates in the Federal Election Commission (FEC) voluntary voting systems standards program. This program defines three levels of testing that voting equipment must pass before it can be used: national qualifications testing, state certification, and local acceptance testing.

National independent testing authorities (ITAs) selected and monitored by the National Association of State Election Directors (NASED) Voting System Board administer the qualifications tests. After ITA certification, any change to either the operating system or the election system requires retesting. A complete description of the qualification tests can be found in the FEC voting system standards section at <http://www.fec.gov>.

After the system has successfully completed qualification testing it is brought to the state for certification testing. Certification testing is conducted by the Secretary of State's office using the following procedure:

- The manufacturer or vendor sends a request for certification in writing to the secretary of state, accompanied by a \$500 fee.
- The secretary of state requires that the equipment be certified by an independent testing authority (ITA). A copy of the ITA's report must be submitted.
- The secretary of state reviews the equipment to ensure that it meets standards established by the Federal Election Commission and the requirements of Kansas law.
- The secretary of state conducts a public meeting in Topeka at which the manufacturer or vendor displays the equipment and members of the Secretary's staff and other interested persons test the equipment.
- The secretary of state may hire a private expert to review the equipment at the manufacturer's expense.
- The secretary of state contacts other jurisdictions in the United States that have certified and used the equipment to inquire about their experiences.
- The secretary of state may grant temporary conditional approval for the equipment to be used in a Kansas jurisdiction before granting final certification.
- If the above conditions are met, the secretary of state makes the final decision whether to grant certification and informs the manufacturer and vendor of the decision in writing.

The final level of tests, acceptance tests, is conducted in the county offices after the voting system has been delivered and installed. The purpose of these tests is to verify that the system as delivered and installed in the county is complete, is working properly, and is identical to the system that was previously qualified by the ITA and certified by the state.

The Help America Vote Act has given the National Institute of Standards and Technology (NIST) a key role in helping to realize nationwide improvements in voting systems by January 2006. NIST's Information Technology Laboratory (ITL) is coordinating the agency's HAVA efforts through its expertise in areas such as computer security and usability. NIST supports the Election Assistance Commission (EAC) as chair of the Technical Guidelines Development Committee (TGDC).

The TGDC makes recommendations to the EAC on voluntary standards and guidelines related to voting machines. As of this writing, NIST has not adopted guidelines or standards.

notes

Conclusion

Adoption of this voting system security policy will increase the overall security of each county's system as well as the security of the electoral process across the state. Further, it will enhance preparation for the deployment of HAVA-compliant voting equipment in the next several years.

-7-

140

**ELECTION CENTER NATIONAL TASK FORCE
ON ELECTION REFORM 2004**

**ELECTION ADMINISTRATION COMMITTEE RECOMMENDATIONS
ON VOTER VERIFIED PAPER AUDIT TRAILS**

The Election Administration Committee will make recommendations on a number of issues including the logic and accuracy testing of voting equipment, the procurement of voting equipment, and early/absentee/satellite voting. The focus of this document though is the committee's feelings on the issue of voter verified paper audit trails (VVPAT) on DRE (Direct Recording Electronic) voting equipment. While a complete report will be included in the final report of the Election Center National Task Force on Election Reform, the committee feels it is important to provide information as quickly as possible as states and federal agencies are discussing this important issue. As we began discussion on this issue, we recognized that some states have already made the decision to move to VVPAT. Other states are just beginning the discussion on this topic and the committee feels it is important to get this information distributed so state legislatures could take our recommendations into consideration when discussing this issue.

The committee was unanimous in stating that all voting systems need the ability for verification that the voters' ballots are recorded and tabulated in accordance with the voters' intent. Whether a paper-based or direct recording electronic voting system, tabulation is conducted electronically and verifiable, documented audit procedures are necessary on all voting systems to insure the integrity of ballot tabulation. For paper-based systems, this audit trail is created by the voter in the form of the marked ballot. For DRE systems, the voter creates an electronic ballot record that needs additional mechanisms to provide verifiability but does not necessarily require a voter verified paper ballot record.

Election administrators currently rely on a combination of an internal audit conducted by the DRE, security procedures and testing to insure the integrity of their voting systems. While these mechanisms have worked well, we feel that confidence in their reliability would be enhanced through increased audit capacity by way of an independent, highly secure, electronic ballot record, not exclusively dependent on the reliability of or "trust" in one vendor's software. Current DRE audit trails have been challenged in, at least, two significant ways: 1) they provide no independent means of verification apart from the operating software provided by the vendor and 2) insufficient protections exist against accidental and irretrievable loss of ballot records.

The Committee makes the following recommendations:

1. National Institute of Standards and Technology (NIST) standards are needed for a scientifically sound, independently verifiable audit trail for DRE systems regardless of whether it involves a contemporaneous paper replica or a tamper proof electronic record. NIST will bring a great deal of independent credibility to this process and standards from this organization will provide the election community with the framework necessary for comprehensive audit trails on all voting systems. The committee feels strongly that these standards should not be a federal mandate but should continue to be voluntary standards for states to adopt.
2. While states may adopt VVPAT, it is the consensus of the committee that a paper audit trail is less accessible, more costly, more burdensome to the voters, more complex for poll officials and less accurate than an electronic audit mechanism. We note that manual tabulation of paper ballots may not be an auditable tabulation process. There are no standards for judging the accuracy of hand counting ballots. Standards developed by NIST can provide future means by which independent verification on DREs can take place.
3. Mandating a paper audit trail would stifle innovation and establish a ceiling on the quality of our verification tools. What is needed is not a ceiling but a floor and room for emerging technologies. Technology is advancing every day and a mandated paper audit trail would lock the vendor community in to that technology and slow development of new, possibly better, audit technology.
4. There are potential serious consequences of a VVPAT system. In addition to significant cost increases, these include lengthened voting times, jammed printers slowing the process and possibly exposing voters' votes, and undermining the Help America Vote Act (HAVA) mandate for blind/visually impaired voters to vote independently. Due to lengthened voting times, more voting devices may be needed which will increase even further the need for additional money.
5. Any DRE paper record that is implemented in a state should be designated as an audit record to be used for verification that the equipment is counting correctly and not be designated as the official ballot. The committee has serious concerns that a paper trail produced by a DRE can be accurately counted. Envision scrolling hundreds of thousands of DRE paper ballots back to an exact race then recounting that race. Also, paper ballots produced by a DRE may be more difficult to securely store than electronic records.
6. Any VVPAT system that is implemented should require retention of the paper ballot at the polling location and must preserve secrecy of the ballot. Allowing paper ballot receipts to leave the polling location could lead to voter fraud and vote buying.

It is the recommendation of the committee that voter verified paper audit trails are unnecessary and will create administrative problems that far outweigh any benefit that they bring. In fact, voters themselves have shown that they do not feel the need for a VVPAT. In exit surveys done in the first major election conducted using VVPAT in the State of Nevada, only 31% of the voters actually used the paper ballot to compare all of the races on their ballot. Without such verification, a VVPAT system cannot provide a scientifically reliable audit of voter intent.

We note that this document is a work in progress and subject to change. It will be included in the Election Center National Task Force on Election Reform final report and is subject to review and approval by the full task force. That final report of the task force will be completed in early March.

The members of this committee thank you for taking the time to consider our thoughts and welcome any questions or comments on our recommendations. Please do not hesitate to contact Dana Walch at (614) 466-6998 if you have any questions regarding this document.

Members:

Dana Walch, Co-Chair, Director of Legislative Affairs, Ohio Secretary of State
Beverly Kaufman, Co-Chair, Harris County, Texas, Clerk
Donald Blevins, Fayette County, Kentucky, Clerk
Ron Cheney, Henrico County, Virginia, Electoral Board Chairman
Bill Cowles, Orange County, Florida, Supervisor of Elections
Pam Finlayson, Allen County, Indiana, Director of Elections
George Gilbert, Guilford County, North Carolina, Director of Elections
James Johnson, Shelby County, Tennessee, Elections Administrator
Conny McCormack, Los Angeles County, California, Registrar-Recorder/County Clerk
Gary Smith, Forsyth County, Georgia, Chairman, Board of Elections
Christopher Thomas, Director of Elections, State of Michigan



CALTECH/MIT VOTING TECHNOLOGY PROJECT

A multi-disciplinary, collaborative project of
the California Institute of Technology – Pasadena, California 91125 and
the Massachusetts Institute of Technology – Cambridge, Massachusetts 02139

SECURITY VULNERABILITIES AND PROBLEMS WITH VVPT

Ted Selker
Media Arts & Sciences, MIT

Jon Goler
MIT

VTP WORKING PAPER
April 2004

Security Vulnerabilities and Problems with VVPT

Ted Selker, PhD Computer Science
Jon Goler

Caltech/MIT Voting Technology Project

April 2004

Abstract

A proposed Voter Verifiable Paper Trail (VVPT) includes a printed ballot as a receipt that a voter can view to verify their vote before leaving an electronic voting machine. This method is also supposed to insure the accuracy of the recorded vote by allowing the tally to be checked later by counting the collected receipts.

This paper considers problems with ergonomics, logistics, security, fraud, and mechanical fragility with using VVPT. Ergonomic problems are introduced by the receipt having a different layout than the ballot, difficulty remembering previous selections to make the verification, by the extra step it introduces after making selections and by it not working well for sightless people. Logistics problems include difficulties in collecting and organizing the receipts, transporting them, and reading and reconciling them with electronic tallies. Security issues include the possibility that receipts can be systematically misprinted in a way that cannot be detected and that hand counting will not easily detect fraud. Mechanical problems include printer breakdowns and supplies running out. VVPTs could add problems by being questioned in various ways or through the development of computer programs that defraud the VVPT systematically. VVPTs do not address existing sources of disenfranchisement such as registration problems, equipment and ballot problems, and polling place problems.

Experiments and elections have yet to establish that people can in fact verify their ballots using a paper receipt. Effective approaches for accurately counting the paper receipts for auditing purposes have not been established either.

Proving that an election correctly records and transmits the intention of the voter is worthwhile. Computers are the first technology that can easily report voting results in multiple formats. Simple systems-verification solutions are possible. Parallel voting and time shifted testing require no extra equipment. Voter Verified Audio Transcripts would simplify voting and improve audit security by presenting verification as feedback during the selection process rather than post hoc auditing.

Introduction

Choosing a government is contentious and the mechanisms for collecting and counting votes have always been on the minds of the people involved. In ancient Greece, Egypt, and Rome people used physical objects, like shards of pottery, to document their choices. Over the last century, developing voting technology has continued to improve the way votes are marked and collected. In 1868 Thomas Edison invented an electronic voting machine. In the 1890s the so-called "Australian secret ballot" was adopted in United States. Hand transcription of marks on paper has given way to automated optical sensors reading the marks. Automated counting reduces the problems of people overlooking, adding, or removing a mark. Writing down columns of local tallies to be added together by hand has given way to spreadsheets and automated calculations. These methods further eliminate human errors. New computer voting machines will not let voters make the mistake of leaving extra marks on alternative selections or making too many selections for a race. Automated processes are eliminating some errors, as well. Prospects are good for using technology to simplify the voting user experience and increasing its accuracy.

However, all technological improvements raise questions and must be implemented in a controlled way. In the case of voting technology, improvements have required experiments, slow rollouts and adjustments. Brazil introduced electronic voting in stages. In 1996, Brazil put electronic voting into place for 40,000 voters with 7% not being able to succeed at recording their votes electronically. Improvements from that experiment allowed this rate to fall to 2% for the 150,000-person experiment 1998. Improvements from that experiment resulted in only an estimated .2% of 106 million voters who were unable to electronically deposit in Brazil in 2000.

User experience problems plagued the early electronic voting machines introduced in this country; in some cases the number of votes that were left unmarked on the new machines was greater than for the equipment they replaced. For example, some electronic ballots placed the selection to scroll to the next race too close to the selection for depositing the ballot, causing some voters to inadvertently cast their ballots before completing it.

In accordance with law, the paper punch cards from the 2000 Florida election have been destroyed. Many people believe that we will never know the intentions of the voters in United States 2000 presidential election. Forensics [1] shows that 2 to 3 percent of the votes were lost due to problems with registration, ballot design and polling place operations. These problems are not new or unusual but are dramatized by the closeness of the 2000 presidential race, coupled with the desire to properly vet its outcome in an information-sophisticated world. These simple-to-solve problems are not being addressed systematically. Instead, the public conversation has shifted to more vague issues of technology in elections and fraud.

The call has gone out for approaches that will produce accurate, secure recording of votes with complete integrity [6]. Unlike paper ballots, voting machines give feedback to voters as they vote. Voting machines that disallow voting for too many candidates have reduced disenfranchisement of voters [7]. The common belief is that electronic voting machines will simplify the vote collection and counting process for all. Historically, the fragmented voting industry consisted of several companies that compete for the occasional upgrade. In the wake of the 2000 election, the Help America Vote Legislative Act of 2002 changed this in that it made available \$1.2 billion in 2003 to upgrade the country's voting machines quickly [3]. Are these monies being released to buy machines when it could be better spent researching how to improve them and the processes in which they are used?

Concerns about security of the collection and counting process have always been important. Computers offer the first technology that can easily make copies of information in different forms for archival preservation. Electronic voting machines of today keep records of the votes on disk, removable physical media in memories and, as a final count, on a paper scroll. These multiple records can improve voting machines' immunity to problems. For example, if a floppy disk from the Brazilian Procom voting machine is unreadable, the election administrator records another one from the internal flash memory in the voting machine.

However, the big question is how can we prove that the selections made on a computer interface by a voter are reflected correctly in the digital voting machine records? Critics of using computers to perform secure operations are speaking up. Broad media coverage has been given to the issue of how we can know that a vote is collected without the computer program tampering with it.

Many approaches to ensure the secure transfer of a voter's selections into the computer are possible [2]. Adequate and provable electronic security could make certain that the vote tallies reflect the voter's intention. A separate Votometer machine can check the voting machine while it is running. Modular architectures can segment the process so that any changes in the votes would take multiple changes to code written by different organizations. Some call for the code being open for anyone to view in a so-called *open source* way. Many believe that separate records that are human readable will be most helpful. Open viewability of a second ballot has seemed attractive to many.

The most popular of these in the public's eye have included Voter Verified Paper Trails (VVPT). The various schemes for this all include a display on which a voter makes selections and a way of viewing a paper receipt that is printed to reflect these selections. The voter cannot take this voting receipt away with them because if they did, it could be used to show how they voted and would compromise the secret ballot and security of elections. Nonetheless, such approaches have captured media and governmental attention as a solution. This paper describes some of the difficulties with VVPTs. A forthcoming paper will describe several alternative verifiable approaches to security.

Ergonomics issues

The VVPT is in a different format than the ballot, in a different place, is verified at a different time, and has a different graphical layout with different contrast and lighting parameters. Handling VVPTs causes other ergonomic

problems for the ballot workers. During the first use of VVPT in an election, in November 2003 in Wilton, CT, virtually all voters had to be prompted to find and verify their receipt. This turned into extra effort for poll workers and extra time for voting. Anything that takes a voters attention away from the act of casting a ballot or causes a voter to invalidate their vote will reduce the chances of them voting for the candidate they intended. Many voters are frightened of going to balloting places because they fear intimidations that actually can transpire. They fear the voting process, the technology, and their registration not being there. The complexity of the voting process is already a deterrent from voting; VVPT adds complexity, which could drive away more voters.

People are extremely good at remembering hundreds of precise images and comparing them against the same image [7]. But the format of the paper receipt will be different than that of the voting machine and because of these differences it is difficult for people to compare them after the fact. Most people have had the experience of taking two columns of numbers and finding it difficult to verify that they have not missed a number. Comparing dozens of selections on a voter-verified paper receipt will take such special care. Complications of comparing a separate paper trail in a different ballot format might add extra difficulty for people with learning and reading disabilities. The Wilton, CT experiment found people not noticing the VVPT because it was in a different place in the booth.

Time limits on voting (3 minutes in New York City) are designed to keep balloting running smoothly. This time will likely need to be extended to allow for checking of the voter-verified paper trail. When people are focusing on a ballot it will be extra work to remember that they have to look at another place to verify their ballot.

When a voter deposits his or her punch card ballot into the ESS PBC 2100, an electronic display shows that the voter has not voted for every race correctly, a paper trail is printed showing exactly the races in which a voter did not vote correctly. This system only shows problems that should be attended to and should be much easier to understand than a paper trail. In watching 500 voters casting ballots, I saw less than one in 10 people who, when they were told they had a problem with their ballot, were actually willing to take a new ballot and vote again. There appeared to be four reasons for this: many said they "knew" they had done the right thing and it must be all right, many felt pressed for time and wanted to leave, some were embarrassed, and some seemed overwhelmed. The task of reviewing the ballot after a person believes they have completed the task can be anticlimactic. One thinks they are done with voting but must go through it again.

The biggest difficulty in verifying a paper trail might be that some jurisdictions have over 100 races on which a voter makes selections. Remembering how one voted on each is difficult. Without a reference guide, it is likely that people who make decisions while marking their vote will forget how they marked the ballot that they are checking. Incorrectly calling fraud on a ballot machine will slow or stop others from getting to vote. In any case the difficulty of the cognitive task of checking a ballot afterwards will be much higher than any perceptual task that is required of the voter while they are marking their ballots [4].

The most popular description of VVPT places it behind glass to avoid losing the integrity of the secondary ballots. To the extent that the paper trail is not directly against the glass or the glass is not thick, offset parallax can make it hard to view. The apparent position of a finger against the glass changes with the viewing angle, making it difficult to accurately see which selection is being verified on a ballot with dozens of races.

Additional ergonomic considerations include lighting and readability issues that probably can be dealt with. For some vision-impaired people magnifying glasses and lighting will not make this process more accessible. A different verification mechanism such as audio verification will be required for them not to be disenfranchised.

The step of reviewing the voting machine after using it has been difficult for voters. In Cook County, IL there are videotapes or machines to train people in using the ESS PBC2100. But, in visiting some 60 precincts, I never saw anyone watch the video. Maybe people believe that they can figure it out once they are in the voting machine.

Ballot worker ergonomic problems exist in the logistics of keeping the receipts secure, counting them, verifying that they are the same number as the number in the DRE, sealing the receipts in a transport box, checking that these are prepared correctly for transport (hopefully under scrutiny of more than one person), and transferring them. Ergonomic problems complicating the process turn into logistical problems.

Logistics problems

Collecting and counting the ballots can be difficult. In Wilton, CT the ballot boxes had a gap through which ballots could have fallen. While watching a precinct close down in Cook County, IL in March 2002, we noticed a ballot on the floor. Transporting ballots has posed problems. Even in LA County, in the last use of punch cards in October 2003, a ballot box was lost for several hours. At 2:00 a.m. somebody had to go look for the hopefully-untampered-with missing box; finally it was found behind a door in the polling place. Ballots have been known to fall off the top of cars and have been left in trunks of cars during transportation. There were allegations in the 2000 election of replacing one set of punch cards in a balloting place with another. Typically a ballot worker transports ballots in a personal car to a collection station. In the fall of 2003 San Francisco election, some ballot workers transported paper ballots in shopping carts down the street. These methods of transportation raise serious concerns on the security of votes.

By the time election workers shut down a polling place, many of them have worked a 13-hour day. In LA County we recently saw a poll worker bully others into saying that they had completed checks that only one person actually did. We saw people closing a ballot box and covering the bar code "for security" which would make it unreadable by the machine as it traveled to the paper ballot collection center. These kinds of mistakes with physical things are always an issue for any system that a person is not familiar with or does not do on a regular basis. When people are doing something that is very important, nervousness as well as fatigue can make them less reliable.

Arranging to store and read the ballots later presents formidable problems. Punch card holes are designed to be the simplest of all possible separate paper records to read in an automated way. While it is easy to read one or ten cards, no one has made a reader that can read a million reliably. Being human readable will make it harder to accurately read the ballots with machines. Even when multiple people read ballots together the tally can change with multiple readings. How many hand counts are required to certify correctness? When the number is different between the paper and the electronic, which one should be trusted? Reading scraps of paper or receipts automatically has not been established as reliable. Machine reading Optical Character Reader (OCR) scan ballots, and punch cards, are more reliable than people reading paper [1]. The suggestion that some human -unreadable indicator, such as a barcode, be included on each receipt compromises the VVPT proponent's goal of the humans as the final judge.

The fact that the VVPT is not the primary election count will be known by the ballot workers likely leading them to be less careful with them than with primary ballots. Since receipts are curled thin paper, the process of counting them at the end of the day is harder than counting paper ballots. Not counting them at poll closing will make it harder to validate later.

Receipts printed with paper tape are hard to stack or organize. In Broward County, FL, for example, the ballots are counted in a warehouse where a loading dock door is commonly left open, letting wind blow in that could shift the paper. VVPTs will require workers to handle scraps of paper curled by the roll in the machine. The mechanical problems of handling the thin paper will be worse than with customary ballots. Interpreting the human readable words on them will be more complex than registering a hole or a filled-in oval.

All election machines today allow an administrator to change the time. Changing the time on the voting machine, ballot, or OCR could allow someone to maliciously revote a precinct. Knowing how many people voted for the day, a dishonest poll worker could fraudulently revote the election. The worker could produce a new fraudulent VVPT, putting into question which VVPT is correct. Luckily this would be a labor-intensive way to defraud an election.

Counting the paper trail presents other problems. Ballot workers arranging and moving cards around always seems precarious. Ballot workers who are running a punch card machine have procedures for dealing with misread cards. Even when everyone is watching in an organized punch card reading operation, people worry about cards getting disorganized, out of order, and being removed or changed.

People are inured to paperwork. People who work with computers constantly have to approve long contracts in order to install software. Computer users are used to approving contracts without reading them completely; most just press the approve button. Conversely, for the non-computer users, the very idea of checking a computer might be confusing; how would they know what to trust? Now consider people who go through checkout lines in the grocery store. When I was a teenager I bought food for my family and had to be frugal. The cashier hand transcribed the

prices into the cash register; I would check my receipt and often find an error; when in my favor, I was refunded. Today cash registers that scan prices have reduced the problems of transcription of the prices and are more reliable. It is not so common to find errors any more and many people do not look at them. ATMs also give receipts. These receipts often have the balance of a bank account and can even indicate the account on them. Even with important financial information on them, these receipts are dropped on the floor or put in the trash can right next to the ATM where anyone could see them. Being surrounded by receipts that we do not pay attention to is an impediment on taking the voter verifiable paper trail seriously. It is unclear that voters will be more careful with a VVPT than they are in caring for their receipts at an ATM or in a grocery store.

Illiteracy can also be a problem when trying to verify a ballot. Variation in formats between the ballot and a verifiable paper receipt can confuse the voter. Voter information often helps people to familiarize themselves with the ballot they will see on the voting machine or to create a crib sheet to allow them to recognize where to mark the ballot. Unfortunately, the paper receipt is in a different format and would require a separate verification sheet to be tested by an illiterate person.

Less than fifty percent of eligible voters in this country vote. The increased logistical problems introduced by VVPT will not make people think voting is easier.

Software Security and Fraud in Voter Verification systems

A natural question about voting concerns possible fraud. David Orr, the county clerk of Cook County, Illinois, said he believes that only 1/3 of voters who are told they have an overvote will take a new ballot. Others have described seeing only one in 10 to one in 30 voters willing to revote when they learned from the ESS PBC2100 receipt that they had spoiled their ballot. Consider that a person decides to commit fraud against a machine with a VVPT. Software could be designed to take advantage of the way voters seldom verify or, even less commonly, act on the information on paper receipts. If the software is designed to print the paper trail incorrectly, some will not notice that there is a problem. Additionally, a line of people will likely be waiting to use the voting machines, and the ballot workers are confronted all day long by people who consider themselves to be disenfranchised by the process so any genuine concern may not be addressed. In the first 10 minutes of watching people vote in LA County, I saw a person give up and decide not to vote because of the line and another person outraged by the procedure for voting when he was not found as a registered voter. Voters want to be helped inside the ballot booth. Voters want to take more time than allowed. Are poll workers able to distinguish these kinds of concerns and concerns stemming from a genuinely defrauded machine?

To defraud a VVPT machine a hacker might make the machine skip a race or appear to have a bad printer, perhaps by making the printer look like it's printing while it's not actually printing anything readable, or simply by making an unreadable section on the receipt. If this unreadable section is carefully printed it will be unreadable in a later recount. This could be used to cover up software defrauding of the electronic vote or it could hide changes in the vote inside the computer.

The vote inside the machine and the vote on the paper could be made to agree or disagree with the electronic vote. In making the VVPT and electronic ballot disagree, the defrauder could be calling into question the quality of technology to create a reason to call for a new election.

In a more likely scenario, the defrauder will change the electronic ballot and depend on the statistics for reading and contesting bad receipts. If a person calls their receipt into question and asks for another receipt to be printed, the hacked VVPT machine can print the "duplicate" receipt correctly, fixing the mistake. By printing the correct receipt when a person asks for it a second time it could literally eliminate the changed ballot, thus eliminating the possibility of detection. Although the program has to give up this one changed ballot it won't happen often. If this follows the experience described above, only one in three to one in 30 people that see a problem will be willing to do something about it. A hacker changing one percent of votes could count on between one in 300 and one in 3,000 voters who see a problem wanting to do anything about it. Considering that up to 1/3 of the fraudulent receipts would be noticed, the hacker has to change one in 75 votes to get a one percent change in the outcome.

If everyone reads their paper receipt carefully, one out of 225 people might notice that their paper receipt is different from their vote. The natural thing is to have the printer reprint it. In a precinct voting 500 people, this will be

noticed twice during the day. When a voter complains and it comes to the attention of one of the several ballot workers that are running the election in a balloting area, it is likely to be caused by the ergonomic problems described above.

If it is because of the fraudulent VVPT, it will likely be the first time the ballot worker encounters this problem, which will make it harder to handle correctly than if they encountered it often. They are likely to encourage the voter to reprint the receipt that would, as outlined above, allow the voting machine to fix the internal count and print the correct receipt to cover up the fraud. If the ballot worker does enter the balloting area where the voter is, in order to verify the legitimacy of a problem with a VVPT, then they would have compromised the secrecy of that ballot. Even if they did enter the voters balloting booth to observe the strangely printed receipt, the natural reaction to an unreadable receipt would be to print a duplicate receipt themselves. Exchanging printers would also reprint the ballot, thereby eliminating the evidence. Shutting down the machine is the only thing that would preserve the fraud to view later, but this would disenfranchise other voters.

As described above, a printer can fake printing problems to cover up changes to the electronic and physical records. By doing this, it can introduce fraudulent tallies. Another way for software to defraud the paper trail is to print more receipts than voters. This could easily be seen as a mechanical problem at the time.

Mechanical problems with VVPT

Voting experts have been concerned about VVPT printers having problems. For instance, the connection between the printer and the machine can be broken, which would stop the printer functioning, and would keep people from being able to vote. If the printer were in the same unit as the voting machine, this problem might be lessened. Unfortunately, that would mean that the voting machine itself would have to be serviced to service the printer. Still it is a separate subsystem and would reduce voting machine reliability.

A printer can break mechanically— the motor, the levers or the solenoids can stop working, for instance. A plug replacement printer could be available, but the problem with the plug replacement printer is whether or not it can pick up where the other one left off. Has one ballot been lost in the meantime? Are we inserting a ballot accidentally when installing a printer? The person replacing a part can read the receipt because it is voter-verifiable. If they do change the paper, do they have access to the printout?

Additionally, the ink can be dried up or run out. If all printers are given new supplies preceding the election and tested, this should not be a problem. However, ensuring that such procedures include signoffs and checks of ink expiration dates is crucial to eliminating ink problems. If the printer is thermal (as many voting equipment printers are), the ink can't dry out. The problem with thermal devices is that heat applied to the paper before or after the election can destroy the printing. Thermal printing also fades with time and the paper tends to deteriorate more quickly.

These issues of printer failure might seem to be minor, but when considering LA County in which 2.2 million people vote in one day, the implications of mechanic problems that can occur are gigantic. In order to add any system that will not increase spoiled ballots, it must not add errors to the system. For the additional paper receipt to complicate the voter experience it must not misprint, jam, run out of paper or ink, malfunction, break, or lose its connection in a way that compromises the secrecy, integrity or accuracy of the vote.

To not lose votes, the printers must be shown to be able to print without failure during a voting election. Each printer must be able to print a typical precinct ballot every election for its planned lifetime. The number of voters in a precinct would not likely be more 200 voters per machine per election. General and special elections typically occur not more than 5 times a year. If the printer is to be used for 10 years a calculation of 15 years of life gives that it should be able to print 15,000 ballots without breaking.

The chance of breaking as opposed to wearing out is different; no machine should break down the day of election in a way that could lose a vote. For LA County, printers would have to have a reliability test that would ensure that they have a mean time between failures that is much larger than 2.2 million.

Alternatives to VVPT

The possible means of improving the authenticity and reliability of software are many. First, better methods for better software development can easily be applied to voting. Modular architecture that separates the different parts of the machine and makes it possible for them to be tracked separately is a good approach. Encrypted votes could improve the validity of the system. Allowing everyone to view the computer program as "open source" is a fashionable approach to ensuring that simple problems in it are not evident.

The "votometer," is a separate system that allows the voter to observe the vote without changing the software. To the extent that a votometer is written by a separate set of people that have no communication with each other, they cannot be in conspiracy to defraud votes. This separate verifying computer can also present the data in exactly the same format as the voting machine. This allows people to compare their votes with a record of those votes in the same format. It can be enhanced by special optics that overlay the two images of the two different displays. Such a votometer system can easily be verified and work across disabilities. The most exciting improvement of votometer over verified paper trails is that reading it is easy, doing it is easy, and establishing its separateness is easy. By solving all of these problems the votometer can literally eliminate the problems of setup and teardown. It can recognize the problems of voting, and establish authentic and separate verifications of the ballot.

Another verification approach is Voter Verified Audio Transcripts (VVAT), which speaks the names of the selections into earphones as selections are made. One advantage of this system is that receiving feedback while a person is making selections is easier to verify than a ballot later. Also, the tape that it produces is easy to count and has better integrity than receipts in a ballot box. Such a system can be implemented with the audio hardware available in today's DRE voting machines.

In the future, many other approaches for establishing verification and audit of votes are possible. Systems could have multiple pieces of software checking each other or multiple computers could verify each other's results. The most exciting of these is a voter's ability to compare his or her vote with the vote stored in the database of the government before they leave the voting booth. This will, in fact, some day be possible. When this is possible not only will we have a qualified belief that the vote this person cast is the vote that is stored in the computer, but we will also have deep security and the knowledge that what occurs at the very front end of the computer in establishing voter intentions is carried through, not only from the registration and authentication, marking the ballot, recording the ballot, storing the ballot, but also to recording the ballot in the election as it is being counted.

We can begin by verifying the votes on parallel machines. Parallel voting consists of pulling a voting machine out of service at random and assigning it to a phantom precinct. By controlling the votes that are cast and checking the results it collects, the machine can show that it recorded them as they were cast, ruling out an extra computer program, a "Trojan horse", "Easter eggs" or other fraud. The voting machine is then used in a real election as a test of its ability to count votes correctly on the day of election thereby establishing the quality of the machines.

Conclusions

This paper shows there are many different ways of disenfranchising a person using a voter-verified paper trail. First, people can be disenfranchised in all the normal ways. They can have registration problems; they can have valid design problems, polling place problems, etc. Second, the paper trail can be lost, stolen, or added to. Third, the equipment can be designed or accidentally set up so it doesn't work, or it slowly changes itself. Finally, intentional fraud can be widespread and created in software in such a way that it can be hidden from the voter and from the ballot worker on the day of election and not be remedied later. The final problem is that counting paper cannot be done at the accuracy level that electronic counting can be done. In this way, even if everything is performed correctly, the difficulty of counting the paper electronically will make it impossible to compare electronic outputs with the paper outputs in a way that can determine whether an accurate count has been achieved.

The Voter-Verified Paper Trail discussion has diverted attention from the main sources of lost votes in past elections. The majority of votes are lost because of problems of registration databases, ballot design, and polling place operations. The force of this discussion is even diverting voting technology development away from improving voting computer architecture. The Voter-Verified Paper Trail has blocked us from establishing standards for improving voting equipment.

Furthermore, VVPT complicates two of the top three problems that have compromised more than one percent of American votes in 2000: equipment problems and polling place operations. It complicates the setup, teardown, and operations of the ballot place. It complicates polling place procedures during the vote. It gives extra and difficult tasks for a person to do and increases the problems with the user experience and the user interface. It also increases the length of time of voting, which makes it, with more steps, easier to make mistakes.

The goal of Voter-Verified Paper Trail—that of establishing a second set of eyes to look at the intentions of a voter—is a worthy one. In fact, ballot design and voting have always been improved by more people looking at the process. In every case improvements in voting have occurred when one person cannot make a decision that changes the vote of another. The idea of establishing a way of doing that is valuable.

We call for improved research in voting technology and for heightened concern over spending large amounts of money on a short-term solution to software hacking problems that have not yet surfaced in elections. Instead, let us focus on verifying the votes in many ways and improving the quality of the whole system.

References;

1. Michael R. Alvarez, Steve Ansolebehere, Erik Antonsson, Jejoshua Bruck, Steve Graves, Thomas Palfrey, Ron Rivest, Ted Selker Alex Slocum Charles Stewart III, Voting - What is, what could be., Caltech/MIT voting project, July 2001
2. Eric Fischer, Election Reform and Electronic Voting Systems (DREs); Analysis of Security issues: CRS Report for Congress, Order Code RL32139 Congressional Research Services Library of Congress, November 4, 2003. <http://www.epic.org/privacy/voting/crsreport.pdf>
3. <http://fecweb1.fec.gov/hava/hava.htm>
4. Roberta Klatsky, Human Memory Structures and processes, Second Edition, W. H. Freeman, San Francisco 1980,
5. Rebecca Mercuri, "A Better Ballot Box?" IEEE Spectrum, Volume 39, Number 10, October 2002.
6. Roy G. Saltman, Accuracy, Integrity and Security in Computerized Vote-Tallying, National Bureau of Standards Special Publications 500-158, August 1988.
7. Roger N. Shepard, Recognition memory for words, sentences and pictures. *Journal of Verbal Learning and Verbal Behavior*, 1967, 6, 156-163. (a)
8. Michael Tomz, Robert VanHouweling, "How Does Voting Equipment Affect the Racial Gap in Voided Ballots? *American Journal of Political Science* 47, no. 1 (January 2003): 46-60.

March 3, 2004

Dear Colleague:

As the principal authors of the Help America Vote Act (Public Law 107-252) (HAVA), signed into law by President Bush on October 29, 2002, we feel compelled to express our concerns about recent legislative efforts that promise enhanced electronic voting system security. Various proposals have been introduced in the House and Senate, but a common feature of these bills is they would amend HAVA to require that all voting systems, including electronic and computer-based systems, produce or accommodate a "voter verified paper record." Not only are such proposals premature, but they would undermine essential HAVA provisions, such as the disability and language minority access requirements, and could result in more, rather than less, voter disenfranchisement and error.

We are certainly aware of the alleged concerns that have been raised in recent months regarding security issues associated with computer-based voting systems and technologies, especially Direct Recording Electronic (DRE) voting systems. These concerns are neither new nor unanticipated by HAVA. To address security-related issues, HAVA creates a Technical Guidelines Development Committee, chaired by the Director of the National Institute of Standards and Technology (NIST), to assist the new Election Assistance Commission (EAC) in developing guidelines and standards to ensure the reliability of the computer technologies being employed in voting systems. These standards will focus not only on the security of computer and network hardware and software and data storage, but also on the detection and prevention of fraud and the protection of voter privacy. Additionally, HAVA provides that the testing and certification of voting system hardware and software must take place in accredited laboratories. NIST initiated this process with a two-day public conference this past December, 2003.

The goal of HAVA is to ensure that every eligible American has an equal opportunity to cast a vote and have that vote counted. HAVA does not mandate the use of DRE systems. It does require, however, that voting systems be enhanced to avoid the errors and accessibility problems associated with antiquated systems, such as punch cards. Computer-based voting systems have a demonstrated track record of achieving this goal, particularly for persons with disabilities. While there are risks associated with any technology, the solution is not to rush to judgment by returning to flawed systems. Rather, the answer is to allow the Commission, together with the active input of election officials, computer experts, and civil rights groups representing voter interests, to develop standards for ensuring the security of all voting systems, as required under HAVA.

The proposals mandating a voter-verified paper record would essentially take the most advanced generations of election technologies and systems available and reduce them to little more than ballot printers. While such an approach may be one way to address DRE security issues, it would, if adopted, likely give rise to numerous adverse unintended consequences. Most importantly, the proposals requiring a voter-verified paper record would force voters with disabilities to go back to using ballots that provide neither privacy nor independence, thereby subverting a hallmark of the HAVA legislation. There must be voter confidence in the accuracy of an electronic tally. However, the current proposals would do nothing to ensure greater trust in vote tabulations but would be guaranteed to impose steep costs on States and localities and introduce new complications into the voting process.

Questions regarding voting systems security, as well as many others, need to be examined by the entity responsible for doing so under existing law, the Election Assistance Commission, before Congress begins imposing new requirements, just months before the 2004 presidential and congressional elections, that have not been fully considered. The security of voting technology is a non-partisan issue. We encourage you to allow HAVA to be implemented as enacted and provide those who are charged with ensuring the security of voting systems the time and flexibility needed to get the job done effectively.

Sincerely,

S/REPRESENTATIVE ROBERT W. NEY

S/REPRESENTATIVE STENY HOYER

S/SENATOR MITCH MCCONNELL

S/SENATOR CHRISTOPHER J. DODD

1-24

Voting Systems Overview

Operations, Security Procedures, and Accountability

Senate Elections & Local Govt.
Date: 1 / 27 / 2005
Attachment 2



January 27, 2005

Presentation to the Kansas
Senate Committee on
Elections and Local
Government

Brian D. Newby
Election Commissioner
Johnson County, Kansas

Discussion Overview

2-2

 **By vote of the people, Johnson County, Kansas has been a voting machine county since 1968, when lever machines were deployed to all voting locations.**

- In 1988, our county became one of the first in the nation to deploy direct record electronic (DRE) voting machines.
- In spring 2002, Johnson County was again one of the first counties in the nation to deploy touch screen voting machines to all voting locations.
- In fall 2004 we upgraded to the latest version of the machines.


 **Today, we will provide a brief summary of:**

- Internal Operation
- Security Procedures
- Election Setup, Operation, and Tabulation
- Touch-Screen System Demonstration
- Audio Ballot Demonstration

Johnson County deploys systematic procedures to assure the security and accountability of all elections.



Internal Operations

 **The Johnson County Election Office is staffed by 16 sworn election professionals who adhere to The Election Center's Code of Ethics, which was adopted by our office in 1997.**

- The Election Office full-time staff manages all aspects of elections for residents of Johnson County.
- The staff is responsible for programming, verifying, tabulating, and controlling every election.
- The vendor has never programmed our elections and does not have remote access to our election software.
- We control our own elections.

 **Our office building, located at 2101 E. Kansas City Road in Olathe, has controlled access and is secured through an alarm system with a numbered lock and password-protected entrance keypad.**

- Within the building there are numerous rooms with different levels of controlled access.
- The election computer room and the ballot storage vault are monitored by security cameras 24 hours a day, 7 days a week.
- Combination lock passwords are changed prior to each election cycle.


Security Procedures


 **The election software computer is freestanding. It is not networked within the office or connected to the Internet.**

1. Physically, the vendor's election software and each individual election database are secured on a computer that is not accessible by our office staff or the vendor's staff.
2. This computer is installed in a secure room with controlled access. The Election Commissioner maintains control of the room keys and no one is admitted without his knowledge. Office policy is that at least two people are in the room at any given time.
3. A video camera also records all activity in this room.
4. Individual election database files are backed up at designated milestones and secured in a fireproof safe. Again, the Election Commissioner maintains control of the keys to the fireproof safe.
5. All voting machine keys, voter cards, and storage media are secured in a controlled access room. Staff maintains a detailed inventory control of these supplies.
6. During elections each machine is housed in a sealed booth within our controlled access building; within the booth, access to the power control and the election results cartridge is controlled within a locked compartment. Again, voting machine keys are secured in a controlled access room.
7. On Election Night, our election results cartridges are hand-carried by election judges to election headquarters.
8. We do not use modems to transmit results.



Accountability of Election Setup

 **The Johnson County Election Office may use only voting systems, equipment and software certified through the Kansas Secretary of State’s Office. The State requires that equipment be certified by the Federal Election Commission (FEC) Voting Systems Standards program.**

 **A voting system must pass three levels of tests before it can be used in Kansas - Federal Qualification Tests, State Certification Tests, and local Acceptance Tests. Our policy is to receive software updates directly from the Independent Testing Authority that certifies the software.**

1. Prior to every election our office conducts a Systems Diagnostic Test on each voting machine to insure that it is operating properly. This test includes evaluation of the printer, card reader, touch screen, power system and battery.
2. Logic and Accuracy (L&A) Tests are performed on each election results cartridge. In addition, an L&A is done to test the integration of the voting machine cartridges with the paper ballot system.
3. This L&A assures the accuracy of the entire process for every election – merging of paper ballot and machine votes to expected hand-calculated outcomes, including a review of all reports.
4. Throughout the entire testing process there is an internal separation of duties and dual sign-off accountability on all processes—maintaining an extensive audit trail, including all proofing documentation.
5. The Election Commissioner has final approval of all proofing and testing material.
6. Each voting machine is secured with a unique padlock and key combination.
7. PC cards for the voting machines are secured at the Election Office until the afternoon before the election, when they are picked up in a numbered, sealed pouch by the Supervising Judge of each polling place.
8. On Election Day, poll workers confirm the seal numbers on PC card pouches and voting machines, then verify protective counters before inserting PC cards into voting machines to activate the election. This validation is signed by all sworn election workers.



Accountability of Operation and Tabulation

 **Each polling place in our county is staffed by sworn election workers, who have attended a mandatory three-hour training session during each election cycle.**

1. The Supervising Judge is responsible for balancing voters processed to votes collected periodically throughout the day. On election day, the Supervising Judge maintains control of all machine keys.
2. There are numerous checks and balances in place, including separation of duties as each voter moves through the polling place.
3. A beginning “zero proof” printout from each voting machine validates that there are no votes stored on the results cartridges. This printout is signed by all sworn election workers.
4. An individual voter receipt is issued to each voter at check-in. A voter must present a voter receipt in order to be issued a voting machine activation card.
5. An activation card is not issued until a voting machine is available for use.
6. Each voter is escorted to a voting machine by a Machine Judge. The Machine Judge validates from the voter receipt that the correct ballot is displayed for the voter.
7. The voter receipt is deposited in an envelope at the voting machine, providing a paper audit trail for the number of votes collected in each voting machine. The voter receipt is comparable to a paper ballot stub.
8. The voter cards are collected at the exit door by an election worker.
9. An end-of-day tally includes balancing voters processed to votes collected, and validating that the numbers of voter cards issued to the polling place are being returned to the Election Office.
10. A closing printout from each voting machine confirms the total number of votes collected in each machine. This printout is again signed by all sworn election workers.
11. The election results cartridges, again secured in a numbered, sealed pouch, are hand-carried by election judges to the Election Office, where the votes are tabulated.

